4-6-2017

Co-design of Security Aware Power System Distribution Architecture as Cyber Physical System

Tarek Youssef
Florida International University, tyous001@fiu.edu

DOI: 10.25148/etd.FIDC001760

FLORIDA INTERNATIONAL UNIVERSITY

Miami, Florida

CO-DESIGN OF SECURITY AWARE POWER SYSTEM DISTRIBUTION ARCHITECTURE AS CYBER PHYSICAL SYSTEM

A dissertation submitted in partial fulfillment of

the requirements for the degree of

DOCTOR OF PHILOSOPHY

in

ELECTRICAL ENGINEERING

by

Tarek Youssef

2017

To: Interim Dean Ranu Jung
College of Engineering and Computing

This dissertation, written by Tarek Youssef, and entitled Co-design of Security Aware Power System Distribution Architecture as Cyber Physical System, have been approved in respect to style and intellectual contents, is referred to you for judgment.

We have read this dissertation and recommend that it be approved.

Mark Roberts

Jason Liu

Sakhrat Khizroev

Arif Sarwat

Osama A. Mohammed, Major Professor

Date of Defense: April 6, 2017

The dissertation of Tarek Youssef is approved.

Interim Dean Ranu Jung
College of engineering and Computing

Andrés G. Gil
Vice President for Research and Economic Development
and Dean of the University Graduate School

Florida International University, 2017

DEDICATION

This dissertation is dedicated to my wife, Eman, whose patience and sacrifice made the completion of this work possible, and to my inspiring parents and sisters, for their supports and prayers.

ACKNOWLEDGMENTS

This dissertation would not have been possible without the help, support, resolute dedication, and patience of my principal supervisor, Professor Osama Mohammed. His passion for success has inspired me to take my own passions seriously, not to mention his advice and unsurpassed knowledge of the various fields of electrical power systems. Professor Mohammed has always provided me an endless supply of ideas, guidance, suggestions, and useful discussions. I am indebted for his enthusiasm, advice, moral as well as financial support, and friendship. I am also grateful for the chance he gave me to work at the Energy Systems Research Laboratory. In this facility, I found all the first-class equipment I needed to experimentally verify my results, and I developed professionally in an environment where work and engineering ethics are highly respected.

I wish to also thank the members of my committee for their support, patience, and valuable discussions. I would like to acknowledge the research support provided from the Department of Electrical and Computer Engineering at Florida International University. I also acknowledge the doctoral dissertation year fellowship from the FIU graduate school during the last period of dissertation research.

Thanks are also due to all the graduate members and undergraduate student scholars at the Energy Systems Research Laboratory, whose discussions, contributions, and assistance helped me achieve my research goals. I am also grateful to the FIU community and department staff.

ABSTRACT OF THE DISSERTATION

CO-DESIGN OF SECURITY AWARE POWER SYSTEM DISTRIBUTION ARCHITECTURE AS CYBER PHYSICAL SYSTEM

by

Tarek Youssef

Florida International University, 2017

Miami, Florida

Professor Osama A. Mohammed, Major Professor

The modern smart grid would involve deep integration between measurement nodes, communication systems, artificial intelligence, power electronics and distributed resources. On one hand, this type of integration can dramatically improve the grid performance and efficiency, but on the other, it can also introduce new types of vulnerabilities to the grid. To obtain the best performance, while minimizing the risk of vulnerabilities, the physical power system must be designed as a security aware system.

In this dissertation, an interoperability and communication framework for microgrid control and Cyber Physical system enhancements is designed and implemented taking into account cyber and physical security aspects. The proposed data-centric interoperability layer provides a common data bus and a resilient control network for seamless integration of distributed energy resources. In addition, a synchronized measurement network and advanced metering infrastructure were developed to provide real-time monitoring for active distribution networks.

A hybrid hardware/software testbed environment was developed to represent the smart grid as a cyber-physical system through hardware and software in the loop

simulation methods. In addition it provides a flexible interface for remote integration and experimentation of attack scenarios.

The work in this dissertation utilizes communication technologies to enhance the performance of the DC microgrids and distribution networks by extending the application of the GPS synchronization to the DC Networks. GPS synchronization allows the operation of distributed DC-DC converters as an interleaved converters system. Along with the GPS synchronization, carrier extraction synchronization technique was developed to improve the system's security and reliability in the case of GPS signal spoofing or jamming.

To improve the integration of the microgrid with the utility system, new synchronization and islanding detection algorithms were developed. The developed algorithms overcome the problem of SCADA and PMU based islanding detection methods such as communication failure and frequency stability. In addition, a real-time energy management system with online optimization was developed to manage the energy resources within the microgrid. The security and privacy were also addressed in both the cyber and physical levels. For the physical design, two techniques were developed to address the physical privacy issues by changing the current and electromagnetic signature. For the cyber level, a security mechanism for IEC 61850 GOOSE messages was developed to address the security shortcomings in the standard.

TABLE OF CONTENTS

CHAPTER			PAGE
Chapter 1		Introduction	1
	1.1	Introduction	1
	1.2	Co-simulation of smart grid as a cyber-physical system	4
	1.3	Smart Grid design challenges	6
	1.4	Integration of distributed energy resources (DER)	7
	1.5	Interoperability challenge	8
	1.6	Communication challenges	8
	1.7	Problem statement	9
	1.8	Research Objective	10
	1.9	Original contribution of this dissertation	11
	1.10	Dissertation organization	16
Chapter 2		Microgrid Cyber-Physical Infrastructure	21
	2.1	Communication requirements for smart grid	21
	2.2	Communication Middleware for Smart Grid Applications	22
		2.2.1 Messages-Centric Middleware Approach	24
		2.2.2 Data-Centric Middleware Approach	27
	2.3	Data Distribution Service Infrastructure for Smart Grid Testbed	30
		2.3.1 System interoperability	31
	2.4	Physical Setup Description and Data Model	34
		2.4.1 Main Grid	35
		2.4.2 System Data Model	36
	2.5	Network Performance	50
	2.6	Summary	55
Chapter 3		Advanced metering infrastructure AMI	57
	3.1	Introduction	57
	3.2	AMI System architecture	58
		3.2.1 Smart Meter	60
		3.2.2 Communication network	61
		3.2.3 Data concentrator	62

3.2.4 Smart meter Head-end 62
3.3 Development of Smart Meter 62
3.3.1 Voltage and current acquisition 64
3.3.2 Signal processing and power calculation 65
3.3.3 Communication Modules 67
3.3.4 Smart meter firmware 68
3.3.5 Development of data concentrator and smart meter Head-end 74
3.3.6 Development of HAN Gateway 75
3.4 Summary 76

Chapter 4 Synchronized measurement network 77
4.1 Introduction 77
4.2 Synchrophasor measurements 78
4.3 Analog interface module 79
4.4 Digital processing modules 80
4.5 Communication Module 87
4.6 Summary 89

Chapter 5 Smart Grid Modeling and Simulation 90
5.1 Introduction 90
5.2 Hybrid simulation toolbox 96
5.3 Protocol Emulation 113
5.4 Remote connection and Micro Grid Intercommunication 116
5.5 Experimental Results 119
5.5.1 Case 1: Generator Synchronization 119
5.5.2 Case 2: Load Sharing 122
5.5.3 Case 3: Topology Reconfiguration 125
5.6 Summary 127

Chapter 6 GPS Based Synchronization Scheme for Distributed DC-DC Converters for Micro Grid application 128
6.1 Introduction 128
6.2 DCMG SYSTEM DESCRIPTION 130
6.3 DC Microgrid voltage and current control. 132

6.4 Synchronization and carrier generation algorithm 134
6.5 PWM carrier generation 139
6.6 Simulation results 141
6.7 Hardware verification and experimental result 143
6.8 Summary 146

Chapter 7 Carrier Extraction Based Synchronization Scheme for Distributed DC-DC converters 148
7.1 Introduction 148
7.2 Carrier frequency and angle extraction 148
7.3 PWM carrier generation 152
7.4 Phase angle control algorithm 155
7.5 Simulation results 158
7.5.1 Case one result 159
7.5.2 Case two: none equal Load sharing 163
7.6 Hardware verification and experimental result 167
7.7 Summary 170

Chapter 8 Microgrid Inverter Based Synchronization and Islanding Detection 171
8.1 Introduction 171
8.2 Conventional SRF-PLL 173
8.3 Adaptive SRF-PLL 177
8.4 Islanding detection and standalone operation 183
8.5 Microgrid control reconfiguration 184
8.6 Simulation results 187
8.7 Experimental results 190
8.8 Summary 194

Chapter 9 Microgrid Energy Management System 195
9.1 Introduction 195
9.2 Real-time communication infrastructure for microgrid control 197
9.3 Intelligent microgrid control 199
9.3.1 Energy management system 199
9.3.2 Advanced Metering Infrastructure and Energy Pricing Mechanism 201

9.3.3 EMS Fuzzy Logic Controller 203
9.3.4 Forecasting 204
9.4 Real Time Online Optimization of Controller Parameters 207
9.5 Security and failover 210
9.6 Results and Discussion 211
9.6.1 EMS performance with real-time pricing scheme 212
9.6.2 EMS performance with TOU pricing scheme 213
9.7 Summary 222

Chapter 10 Load Signature and Customer Privacy 223
10.1 Introduction 223
10.2 Harmonic and reactive current extraction 226
10.2.1 Synchronous Reference Frame Current Reference Generation Method 227
10.2.2 Instantaneous Power Theory reference generation method. 228
10.2.3 Proposed current Reference Generator 229
10.2.4 Active power filter current controller. 231
10.3 Case studies 233
10.3.1 Case Study one: Three phase dynamic inductive load. 234
10.3.2 Case Study two: Three phase unbalanced inductive load. 235
10.3.3 Case Study three: Three phase nonlinear load with harmonic current 236
10.3.4 Case Study four: Emulating a nonlinear load current signature 236
10.4 Summary 244

Chapter 11 Electromagnetic Signature 245
11.1 Introduction 245
11.2 Harmonic Reductions of Electric Drives 248
11.2.1 Hardware Solutions (Filters): 248
11.2.2 PWM Modifications: 249
11.3 Harmonic Behaviors of Stray Fields 250
11.4 Control and Optimization Procedure 252
11.5 Harmonic Suppression, Discussion, and Results 257
11.5.1 Sinusoidal PWM 257

11.5.2 SPWM Harmonics Manual Suppression 260
11.5.3 SPWM Harmonic Automatic Suppression 263
11.5.4 SVPWM 266
11.5.5 SVPWM Harmonic Manual Suppression 266
11.5.6 SVPM harmonic Automatic Suppression 267
11.6 Summary 270

Chapter 12 IEC 61850 Security Analysis 272
12.1 Introduction 272
12.2 IEC 61850 Overview 276
12.3 IEC 61850 security 280
12.4 MMS vulnerabilities 280
12.5 GOOSE Message analysis and vulnerabilities. 282
12.6 IEC 62351 Security Standard 287
12.7 Implementation vulnerability 289
12.8 Summary 292

Chapter 13 Sequence Hopping Security Mechanism For Energy Systems 294
13.1 Introduction 294
13.2 GOOSE messages vulnerabilities and attack surface 295
13.3 Sequence hopping security mechanism 297
13.3.1 Message sequence synchronization and monitoring server (MSSMS)…. 299
13.3.2 PRNG synchronization process 300
13.3.3 SSL encryption 301
13.4 Experimental validation 305
13.5 Summary 312

Chapter 14 Conclusions and Recommendation for Future Work 314
14.1 Conclusions 314
14.2 Recommendations for Future Works 318

References 320

VITA..... 333

LIST OF TABLES

TABLE PAGE

Table 2.2-1. Objects and topics list. Photovoltaic: PV 38

Table 2.2-2. Quality of Service.....49

Table 2.2-3. DDS performance for 32 bytes messages size 52

Table 6-1: DC-DC boost converters parameters.....132

Table 9-1: Total Savings.....213

Table 11-1: Details of the Components in the Testbed Setup 259

Table 12-1: Compliance Test Results. 292

LIST OF FIGURES

FIGURE PAGE

Figure 2.1. C38.118 message frame....25

Figure 2.2. Middleware approaches: (a) message-centric; and (b) data-centric adapted from [54] 28

Figure 2.3. DDS applications vs different communication standard 32

Figure 2.4. DDS vs OPC middleware 33

Figure 2.5. Schematic diagram for the smart grid testbed 34

Figure 2.6. Generators data structure and pub/sub example 40

Figure 2.7. DDS testbed infrastructure. 40

Figure 2.8. The developed data distribution service (DDS) data acquisition (DAQ) and controller block diagram 41

Figure 2.9. (a) Unicast communication; and (b) multicast communication 47

Figure 2.10. a-Performance test for DDS unicast and best effort quality of service b-Performance test for DDS unicast and reliable quality of service (QoS) 53

Figure 2.11. a- Performance test for DDS multicast and best effort QoS. B-Performance test for DDS multicast and reliable QoS 54

Figure 3.1: Smart meter infrastructure architecture 59

Figure 3.2: Smart meter block diagram 60

Figure 3.3: smart meter digital processing and communication board 63

Figure 3.4: current and voltage transducers connection diagram 64

Figure 3.5: Energy computing DSP engine connection diagram 66

Figure 3.6: Power line modem block diagram 67

Figure 3.7: Smart meter firmware architecture 69

Figure 3.8: STMPC1 data record 73

Figure 3.9: smart meter head-end interface 74

Figure 3.10: Data flow between customer and utility domains 75

Figure 4.1: Phasor measurement unit general block diagram.....79

Figure 4.2: analog filter schematic diagram 81

Figure 4.3: analog filter frequency response.....82

Figure 4.4: Analog comparators 82

Figure 4.5: Digital processing board block diagram.....83

Figure 4.6: Phase comparison with the GPS reference (a) zero degree phase shift, (b) 180 phase shift, (c) 90-degree phase shift.....84

Figure 4.7: Phase detection timing diagram, (a) lag signal, (b) lead signal.....86

Figure 4.8: Synchronized measurement test setup.....88

Figure 5.1: Hybrid Smart Grid Testbed Block Diagram.....94

Figure 5.2: Testbed LabVIEW Interface 95

Figure 5.3: Domain Creator. 97

Figure 5.4: Multiple Domain Creators with Multiple IDs 97

Figure 5.5: Generator Control Block 98

Figure 5.6: Generator Control Block Parameters 99

Figure 5.7: Serial Interface Board.....99

Figure 5.8: Interface Board Block Diagram 100

Figure 5.9: Circuit Breaker Block Diagram.....101

Figure 5.10: Load Control Block 102

Figure 5.11: Busbar Block 102

Figure 5.12: Transmission Line Block.....103

Figure 5.13: Hybrid Microgrid Block Diagram.....104

Figure 5.14: Microgrid Control Block 105

Figure 5.15: Smart Meter Block 105

Figure 5.16: Energy Storage Control Block 106

Figure 5.17: HIL implementation using DDS and the developed interface library 108

Figure 5.18: The hierarchy of the developed automatic controller for the smart grid testbed 109

Figure 5.19: Slack generator control 109

Figure 5.20: Slack generator control connection 110

Figure 5.21: Synchronization Controller 110

Figure 5.22: Power controlled generator control 111

Figure 5.23: PQ generator controller connection 111

Figure 5.24: Main automation and startup controller 112

Figure 5.25: Block Diagram for IEC 61850 113

Figure 5.26: IEC 61850 and DDS publisher/subscriber functions 114

Figure 5.27: complete configuration for the testbed with remote connection capability 116

Figure 5.28: Testbed remote access domains 117

Figure 5.29 Routing service intermediate domain 118

Figure 5.30: Experimental results, voltage, frequency and synchronization switch status (a) Generator 1 frequency; (b) Generator 2 frequency; (c) Generators Voltage; and (d) Generators Power 121

Figure 5.31: Synchronization Process 122

Figure 5.32: Case 2, load sharing. Power of (a) load; (b) generator 1; (c) generator 2; (d) generator 3; and (e) generator 4 124

Figure 5.33: Case 3, topology reconfiguration. (a) Output power of generators 1 and 2; (b) load 4 power; and (c) load 4 voltage 126

Figure 6.1: Distributed DC-DC converters connected to common DC bus 131

Figure 6.2: ALLC voltage and current control scheme 132

Figure 6.3: ALLC current control scheme 133

Figure 6.4: Frequency multiplier using PLL 135

Figure 6.5: Digital phase locked loop DPLL 136

Figure 6.6: DPLL SIMULINK Simulation Block Diagram 137

Figure 6.7: Propose DPLL simulation performance 138

Figure 6.8: Synchronized PWM carrier generation 139

Figure 6.9: Phase adjustment simulation model 140

Figure 6.10: carrier phase adjustment performance 140

Figure 6.11: Multiple converters synchronization performances (a) DC bus voltage, (b) ripple RMS, (d) carrier 1 phase angle, (e) carrier 2 phase angle 142

Figure 6.12: the GPS software control panel 143

Figure 6.13: 1PPS and high-frequency output signal 144

Figure 6.14: Hardware setup for the GPS carrier synchronization 145

Figure 6.15: DC bus voltage with adjustable carrier phase angles 146

Figure 7.1: Harmonics content of DC-DC boost converter output. (a) 2 KHz switching frequency, (b) 4 KHz switching frequency 149

Figure 7.2: DC bus carrier frequency and magnitude extraction algorithm block diagram 151

Figure 7.3: Phase locked loop and peak detector output. (a) DC bus voltage, (b) bandpass filter output, (c) estimated frequency, (d) carrier phase angle, (e) master carrier 152

Figure 7.4: PWM carrier generation block diagram 153

Figure 7.5: synchronized carrier generation. (a) Master carrier, (b) master carrier phase angle, (c) converter's 2 carrier, (d) converter's 3 carrier 154

Figure 7.6: Multiple converters with carrier extraction and PSCA block diagram 155

Figure 7.7: Search algorithm state machine 157

Figure 7.8: Perturb and observation search space 158

Figure 7.9: Case1 simulation results for Equal load sharing. (a) DC bus voltage ripple, (b) Ripple Magnitude, (c) Phase offset1, (d) Phase offset 2 160

Figure 7.10: carriers phase angle for case one. (a) Carriers at t=0 s, (b) Carriers at t=2.5 s, (c) Carriers at t=3.5 s, (d) Carriers at t=5.5s 161

Figure 7.11: harmonics analysis for case 1. (a) Harmonics magnitude before PSCA, (b) Harmonics magnitude after PSCA 162

Figure 7.12: Case2 simulation results. None Equal load sharing. (a) DC bus Voltage, (b) Ripple Magnitude, (c) Phase offset 1, (d) Phase offset 2 164

Figure 7.13: carriers phase angle for case two. (a) Carriers at t=0.5 s, (b) Carriers at t=1.5 s, (c) Carriers at t=2.5 s.....165

Figure 7.14: harmonic analysis for case 2. (a) Harmonics magnitude before PSCA, (b) Harmonics magnitude after PSCA 166

Figure 7.15: Hardware setup for carrier extraction and PSCA verification 167

Figure 7.16: Low processing overhead frequency and phase estimator 168

Figure 7.17: DC bus voltage with PSCA. 169

Figure 7.18: Three converter carriers after PSCA 169

Figure 8.1: Conventional SRF-PLL.....173

Figure 8.2: SRF-PLL Phase angle and estimated frequency under unbalanced voltage condition. (a) Three phase voltage. (b) Phase angle. (c) Estimated frequency.....175

Figure 8.3: SRF-PLL Phase angle and estimated frequency under distorted voltage condition. (a) Three phase voltage. (b) Phase angle. (c) Estimated frequency.....176

Figure 8.4: Moving average filter frequency response 177

Figure 8.5: Butterworth low pass filter frequency response.....178

Figure 8.6 Proposed ASRF-PLL with an adaptive moving average filter simulation model.....180

Figure 8.7: ASRF-PLL Phase angle and estimated frequency under unbalanced voltage condition. (a) Three phase voltage. (b) Phase angle. (c) Estimated frequency.....181

Figure 8.8: ASRF-PLL Phase angle and estimated frequency under distorted voltage condition. (a) Three phase voltage. (b) Phase angle. (c) Estimated frequency.....182

Figure 8.9: SIMULINK model for islanding detection algorithm. 184

Figure 8.10: SIMULINK model for proposed ASRF-PLL with islanding detection algorithm and internal frequency reference 184

Figure 8.11: Reconfigurable converter control 185

Figure 8.12: Microgrid Block diagram 186

Figure 8.13: Microgrid performance with conventional SRF-PLL. (a) three phase voltage. (b) Estimated phase angle. (c) Estimated frequency. (d) Grid status 188

Figure 8.14: Microgrid performance with ASRF-PLL. (a) three phase voltage. (b) Estimated phase angle. (c) Estimated frequency. (d) Grid status 189

Figure 8.15: Microgrid test bed. 190

Figure 8.16: Conventional SRF-PLL experimental results. (a) phase voltage, (b) Phase angle, (c) frequency 191

Figure 8.17: Proposed ASRF-PLL experimental results 192

Figure 8.18: ASRF-PLL islanding detection 193

Figure 9.1: Proposed DDS Network and Microgrid Logical Control Hierarchy 198

Figure 9.2: Overall System Topology 200

Figure 9.3: Real-Time Pricing Algorithm 202

Figure 9.4: Energy Transactions Logic 206

Figure 9.5: Performance of neural network (a) with persistence QoS (b) without persistence QoS 206

Figure 9.6: Optimization Process 208

Figure 9.7: Constrained Search Space for Trapezoidal Membership Functions 208

Figure 9.8: Failover Mechanism 211

Figure 9.9: Winter Real-time Pricing without Optimized Parameters 214

Figure 9.10: Winter Real-time Pricing with Optimized Parameters 215

Figure 9.11: Summer Real-time Pricing without Optimized Parameters 216

Figure 9.12: Summer Real-time Pricing with Optimized Parameter 217

Figure 9.13: Winter TOU Pricing without Optimized Parameters 218

Figure 9.14: Winter TOU Pricing with Optimized Parameters 219

Figure 9.15: Summer TOU Pricing without Optimized Parameters.....220

Figure 9.16: Summer TOU Pricing with Optimized Parameters.....221

Figure 10.1: shunt active power filter block diagram 225

Figure 10.2: Block diagram of synchronous reference frame reference generation method.....228

Figure 10.3: Block diagram of Instantaneous Power Theory reference generation method.....229

Figure 10.4: A block diagram of the reference current generator.....230

Figure 10.5: Voltage source inverter with self-supported DC bus 232

Figure 10.6: A block diagram of the developed hysteresis controller 233

Figure 10.7: APF hardware setup 234

Figure 10.8: Three phase dynamic load with shunt APF connection diagram 235

Figure 10.9: APF performance with the three-phase dynamic load. (a) Supply voltage, (b) Load current, (c) Supply current 237

Figure 10.10: Dynamic load and supply current phase angle. (a) Supply voltage, (b) Load current, (c) Supply current.....238

Figure 10.11: APF performance with three phase unbalanced load. (a) Supply voltage, (b) Load current, (c) Supply current 239

Figure 10.12: Unbalanced load and supply current phase angle. (a) Supply voltage, (b) Load current, (c) Supply current 240

Figure 10.13: APF performance with three phase non-linear load. (a) Supply voltage, (b) Load current, (c) Supply current 241

Figure 10.14: nonlinear load and supply current phase angle. (a) Supply voltage, (b) Load current, (c) Supply current.....242

Figure 10.15: Load signature emulation. (a) Supply voltage, (b) Load current, (c) Supply current.....243

Figure 11.1: Schematic of the test setup (PWM VSI drive) 250

Figure 11.2: The procedure of the controller.....253

Figure 11.3: Digital oscillator scheme 255

Figure 11.4: Spectrum analysis procedure 256

Figure 11.5: Magnetic field intensity (H) of the induction motor connected to the drive using the SPWM technique 258

Figure 11.6: (a) Setup inside the enclosure (the converter and the motor) and (b) control and monitoring setup. Note that the antenna is located 12 in away from the center of the machine (~3 inch from the cage) 260

Figure 11.7: Block diagram of the sinusoidal PWM with harmonic compensation block 262

Figure 11.8: Magnetic stray field intensity (H) of induction motor using SPWM with and without HSC for second harmonic suppression 262

Figure 11.9: Magnetic stray field intensity (H) of induction motor using SPWM with and without HSC for fourth harmonic suppression 263

Figure 11.10: Magnetic stray field intensity (H) of induction motor using SPWM with and without HSC for fifth harmonic suppression 263

Figure 11.11: Automatic harmonic suppression block diagram 265

Figure 11.12: State machine tracking algorithm 265

Figure 11.13: Magnetic stray field intensity (H) of induction motor using SPWM with and without HSC for fourth harmonic suppression in automatic mode 266

Figure 11.14: Block diagram of the SVPWM with harmonic compensation block 268

Figure 11.15: Magnetic stray field intensity (H) of induction motor using SVPWM with and without HSC for fourth harmonic suppression 268

Figure 11.16: Magnetic stray field intensity (H) of induction motor using SVPWM with and without HSC for fifth harmonic suppression 269

Figure 11.17: Magnetic stray field intensity (H) of induction motor using SVPWM with and without HSC for simultaneous fourth and fifth harmonic suppression 269

Figure 11.18: Magnetic stray field intensity (H) of induction motor using SVPWM with and without HSC for fourth harmonic suppression in automatic mode 270

Figure 12.1: Substation automation using serial data 274

Figure 12.2: IEC 61850 substation automation. 275

Figure 12.3: Direct connection of instrumentation devices without process Bus.....275

Figure 12.4: Connection of instrumentation devices with merging units and process Bus 276

Figure 12.5: IEC 61850 data model.....277

Figure 12.6: IEC 6180 ACSI protocol mapping.....278

Figure 12.7: substation automation system designs and configurations process based on SCL 279

Figure 12.8: ARP Cache Poisoning Mechanism.....281

Figure 12.9: Structure of a GOOSE Datagram.....282

Figure 12.10: Adaptive GOOSE transmission time.....285

Figure 12.11: Spoofed GOOSE message attack 286

Figure 12.12: Goose messages with two different stNum 290

Figure 12.13: Outdated GOOSE message content.....291

Figure 13.1: Sequence hopping security mechanism block diagram.....298

Figure 13.2: Publisher synchronization flowchart.....302

Figure 13.3: Subscriber synchronization flowchart.....303

Figure 13.4: Root certificate 304

Figure 13.5: Client and server certificates 304

Figure 13.6: embedded sequence hopping security solution test setup. 306

Figure 13.7: End-to-end delay time for the embedded sequence hopping implementation. 306

Figure 13.8: Bump in the wire sequence hopping security mechanism implementation setup. 307

Figure 13.9: MSSMS server and client outputs during SSL initialization. 308

Figure 13.10: SSL handshaking.....309

Figure 13.11: Original GOOSE message.....310

Figure 13.12: GOOSE message with HseqNum field 311
Figure 13.13: Bump in the wire solution end-to-end delay 312

LIST OF ACRONYMS

ACRONYMS	DETAILS
ACSI	Abstract Communication Service Interface
ALLC	advanced Lead-Lag Controller
AMI	Advanced Metering Infrastructure
APF	Active Power Filter
API	Application Programming Interface
ARP	Address Resolution Protocol
BPF	Band Pass Filter
CA	Certificate Authority
CB	Circuit Breaker
CDC	Communication Device Class
CID	Configured IED Description
CIM	Common Information Model
CORBA	Common Object Request Broker Architecture
CP	Current Price
CP-PLL	Charge Pump PLL
CPS	Cyber-Physical System
CSMA	Carrier Sense Multiple Access
CTs	Current Transformers
DAQ	Data Acquisition
DDS	Data Distribution Service

DEI	Drop Eligible Indicator
DER	Distributed Energy Resources
DG	Distributed Generation
DMIPS	Dhrystone Million Instructions Per Second
DPLL	Digital Phase Locked Loop
DS	Direct Digital Synthesizer
EDF	Earliest Deadline First
EMI	Electromagnetic Interference
EMS	Energy Management System
FC	Fuel Cell
FIR	Finite Impulse Filter
FLD	Forecasted Load Demand
FPL	Florida Power and Light
GDS	Global Data Space
GOOSE	Generic Object Oriented Substation Event
GPS	Global Positioning System
HAN	Home Area Network
HIL	Hardware In the Loop
HPF	Highest Priority First
HSC	Harmonics Suppression Controller
ICD	IED Capability Description
IEC	International Electrotechnical Commission

IED	Intelligent Electronic Device
IF	Intermediate Frequency
IGMP	Internet Group Management Protocol
ISO	International Organization for Standardization
JADE	Java Agent Development
JMS	Java Messaging System
LB	Lower Bounds
LD	Logical Device
LON	Local Operating network
LPF	Low Pass Filter
MAC	Media Access Controller
MMS	Manufacturing Messaging Specification
MPI	Message Parsing Interface
MSSMS	Message Sequence Synchronization and Monitoring Server
NAN	Neighbor Area Network
NHP	Next Hour Price
NILM	Non-intrusive Load Monitoring
NSWC	Naval Surface Warfare Center
OMG	Object Management Group
OpenFMB	Open Field Message Bus
OTP	One Time Programming
PCC	Point of Common Coupling

PCP	Priority code point
PD	Physical Device
PDC	Phasor Data Concentrator
PDUs	Protocol Data Unit
PLC	Power Line Communication
PLL	Phase Locked Loop
PMU	Phasor Measurement Unit
PRNG	Pseudo Random Number Generator
PRU	Programmable Real-time Unit
PSCA	Phase Shift Control Algorithm
PSO	Particle Swarm Optimization
PV	Photovoltaic
PWM	Pulse Width Modulation
QoS	Quality Of service
RF	Radio Frequency
RISC	Reduced Instruction Set Computing
RMP	Resource Management and Protection
RR	Round-Robin
RT-CORBA	Real-Time Common Object Request Broker Architecture
RTI	Real-time Innovation company
RTPS	Real Time Publisher-Subscriber
RTSJ	Real-Time specification for Java

RTU	Remote Terminal Unit
SBC	Single Board Computer
SCADA	Supervisory Control And Data Acquisition
SCD	Substation Configuration Description
SCL	Substation Configuration Language
SFR-PLL	Synchronous Reference Frame Phase Locked Loop
SGIP	Smart Grid Interoperability Panel
SIL	Software In the Loop
SMV	Sampled Measured Values
SoC	State Of Charge
SPI	Serial Peripheral Interface
SPWM	Sinusoidal Pulse Width Modulation
SRF	Synchronous Reference Frame
SSD	System Specification Description
SSL	Secure Socket Layer
SSM	Small-Signal Model
SVPWM	Space Vector Pulse Width Modulation
THD	Total Harmonic Distortion
TID	Tag Control Identifier
TLS	Transport Layer Security
TOU	Time Of Use
TPID	Tag Protocol Identifier

UART	Universal Asynchronous Receiver/Transmitter
UB	Upper Bounds
UTC	Coordinated Universal Time
VCO	Voltage Controlled Oscillator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VSI	Voltage Source Inverter
VTs	Voltage Transformers
WAMS	Wide Area Measurement System
WAN	Wide Area Network
WECS	Wind Energy Conversion System
XML	Extensible Markup Language

Chapter 1 Introduction

1.1 Introduction

The increased penetration levels of renewables and distributed energy resources result in increased challenges in maintaining reliable control and operation of the grid [1]. Integrating a wide variety of systems governed by different regulations and owned by different entities to the grid increases the level of uncertainty, not only on the demand side but also in terms of generation resource availability [2]. This complicates the process of achieving generation/demand balance. Renewable energy sources vary by nature and require intelligent forecasting and prediction systems to determine how and when this energy can be used [3]-[5]. Most of these distributed resources will be installed on the distribution network, which already in its current state lacks the proper communication and control network necessary to control the applicable resources [6],[7]. Moreover, the large number and widespread use of these resources makes controlling them from a central location difficult [8]. To overcome these problems, deep integration between intelligent measurement nodes, communication systems, information technology, artificial intelligence, power electronics and physical power system components must be made to manage the smart grid resources [9]. On the one hand, this type of integration can dramatically improve the grid performance and efficiency, but on the other, it can introduce new types of vulnerability to the grid. The risk of vulnerability escalates when the level of integration between the physical and cyber components of the power system increases [10].

The security threats to the grid due to deep integration with cyber components are significant and widespread, taking on various forms ranging from compromising smart meters to attacking wide area monitoring system (WAMS) and generation control system [11],[12]. The transmission system and substations represent the backbone for the grid. Attacking the substation automation systems could lead to severe damage and blackout [13],[14].

Considering this type of potential issue in the original design will lead to a more optimum design for cyber and physical components, ensuring continuity of service and system resiliency under various types of events and/or attacks. The design and optimization of such complex systems requires coordination between the cyber and physical components in order to obtain the best performance while minimizing vulnerability risk. The challenge is not only how to design the new secure cyber-physical system, but the transition from current systems to the new design is another challenge. Most of the installed components utilize older protocols and will last for decades [15]. It is necessary to consider the interoperability between current and legacy component in the design of the new system [16],[17].

For the co-design of such a complex system, first, the interaction between cyber and physical component needs to be identified. The power system control uses different types of measurements and feedback signals. The impact of compromising these types of the signal on the power system stability should be identified to define the level and type of security required for each type of signal. An integrated modeling and simulation framework that presents an integrated model for cyber and physical components is

required to study this interaction and the impact of different types of vulnerabilities on the system stability.

Smart grid systems could be affected by different types of vulnerabilities from different sources. The first source of vulnerabilities come from lacking security measures and data integrity checks in old protocols, control tools, and software tools. For example, Most of the protocols used in WAMS and substation automation, such as IEEE C37.118, were designed for efficiency and don't have any security measures [15],[18],[19]. Even for new protocols that specify some security measures, such as IEC 62351 standard, the control and operation requirements possess some restriction on applying these measures. As an example, the encryption is not supported for GOOSE messaging, which operates at Layer 2 to meet the performance and 4ms maximum delay restriction [20]. The second source of vulnerabilities could result from miss-configured systems and components. Miss-configured equipment, such as default accounts, open ports, etc. can leave the back door open for an attacker. The last source of the vulnerability is the software and implementation bugs [15]. Even if the system utilizes a strong security standard, encryption and authentication mechanism, undiscovered software bugs can lead to dangerous security threats. For example, the famous heart bleeding bug that affects a large percentage of secured web servers that use OpenSSL server was related to an implementation bug. In this particular case, the problem was not related to the Secure Sockets Layer (SSL) standard or the encryption algorithm [21]. The bug comes from the software implementation of OpenSSL server. The affected servers have a buffer overflow software bug, which allows the attacker to obtain security keys and certificates [22].

Since the vulnerability of the system could result from system protocols, implementation or particular hardware equipment, the integrated modeling and co-simulation framework should be equipped with hardware in the loop (HIL) and software in the loop (SIL) capabilities to test the actual components and firmware related vulnerabilities.

1.2 Co-simulation of smart grid as a cyber-physical system

The concept of co-simulation has been introduced. In[23], co-simulation is described as the process of integrating two software packages together and providing synchronization among them. As an example, [23] proposed the integration of Simulink, which is concerned with modeling the physical system's dynamic behavior, with Omnet++, which is concerned with modeling the communication network behavior, to develop smart grid applications. Similarly, in [24] a co-simulation framework was developed by combining OpenDSS and Omnet++ for power system and communication networks simulations in order to investigate wide area smart grid monitoring systems. The work in [24] focused on the time synchronization between the solvers for the aforementioned software packages. Authors in [25] argued that there is a large gap in the area of simulating cyber-physical systems, which relies on having the communications and control working as intended and more effort needs to be put in the co-simulation area. For that, they introduced an event-driven co-simulation module based on the OpenDSS and Network Simulator NS2. MATLAB was used for the coordination of events. A co-simulation platform of a low-voltage grid based on IEC 61850 was presented in [26], where MATLAB's SimPowerSystems and SimEvents toolboxes were

used to model the system's physical and cyber information flow, respectively. There are many other similar efforts in the literature which rely only on simulation software modules. These systems represent an important step towards properly modeling the cyber and physical domains of a cyber-physical system. Nonetheless, these simulators are not implemented over a real communication network. Therefore, they will not be able to account for practical issues with high fidelity, as they are limited with the functionalities provided in the network simulation software, which most of the time is proprietary. For instance, network simulators do not work on the packet level; they usually model networks on the large scale and use statistical and probabilistic models to predict delays. Also, practical issues due to different firmware implementations cannot be realized in network simulators. Two Ethernet switches from different vendors might have a different implementation to which specific vulnerabilities can be analyzed and found. Such simulation environments usually have their solvers synched and do not operate in real-time and therefore cannot be easily interfaced with actual hardware and intelligent electronic devices (IED).

From another perspective, there are several works that included hardware modules in the loop of the simulation platforms. Here, there are two methodologies: (1) is integrating power equipment, such as generators, actuators, converters, etc, into the simulation environment to test control algorithms on real hardware, whereas (2) is network design and testing by integrating IEDs and other embedded devices with traffic generation software packages. A hardware in the loop simulation testbed for distributed microgrid management based on multi-agent systems was presented in [27]. The presented system

is based on the Zigbee protocol and the simulation and hardware were integrated through an I/O conditioning board. This approach is limited to the specific application it was developed for and is hard to expand to include various smart grid applications. Also, in [28] actual Phasor Measurement Units (PMUs) were integrated with a real-time digital simulator via an IEC 61850 bus to model passive islanding schemes. Although an actual IEC 61850 network was integrated with the simulations, this implementation is application specific and is hard to expand and manage the complex communication requirements for other smart grid applications. In a pure networking perspective, [29] proposes a method for testing intelligent devices' communications in distributed systems. This platform is interesting since it incorporates several protocols, such as IEC 61850, DNP3, IEC 61870-5, IEC 61870-6 (ICCP/Tase.2), and Modbus. However, the integration of these protocols is based on a proprietary Distributed Test Manager and therefore is not easily expandable and requires special libraries to interface with other simulation tools. Both modeling approaches do not provide a comprehensive framework for properly modeling cyber-physical systems and most importantly the interactions between them. Also, the second approach (2) is usually concerned with a single or a few protocol combinations and will require a lot of engineering and programming effort to integrate different applications and devices together.

1.3 Smart Grid design challenges

Several technical challenges need to be identified and addressed during the design of the smart grid architecture. These challenges are spread over a multidisciplinary area

including communication, control, and power system. These challenges can be classified as below.

1.4 Integration of distributed energy resources (DER)

Smart grid is characterized by large penetration of distributed and renewable energy resources. High penetrations of renewable energy increase the uncertainty of generation resource availability. Moreover, most of these resources will be installed on the distribution side. Current grid control model was designed to control a few generation stations from centralized control systems. Applying the existing control model for distributed energy resources, taking into account large geographic area and the amount of data needed to be transferred to control centers possesses large technical and economic challenges. The technical challenges are associated to design the communication system that covers the large geographic area and transfers huge amounts of raw measurements and control signals. The processing power needed to process this information and take the necessary action in real time is another challenge. Implementation of such control and communication network will be costly.

Moreover, the centralized control model suffers from the reliability and single point of failure problems. Failure of a centralized server or communication channel may lead to severe system problems. To solve these issues, the control model should be changed from centralized control to decentralized control model. Instead of a centralized control center, which collects and process all information locally, the system will be divided into a number of subsystems with a local intelligent controller. The local controller will process the data locally and perform the necessary control action in their area. Neighbor's area

controllers will be able to exchange the information to coordinate the operation in the local area and support the overall system stability. Only high-level data and control command will be needed to be transferred between intelligent controllers and control centers. By processing the data locally and performing local control actions, the amount of data transfer and communication bandwidth will be reduced. The required processing power on control centers will be less and the system reliability will be improved by avoiding a single point of failures.

1.5 Interoperability challenge

Integrating a wide variety of systems governed by different regulations and owned by different entities to the grid possesses an interoperability challenge. Several protocols and standard were developed for smart grid operation, such as DNP3 for process automation and SCADA systems, IEC61850 for substation automation, C37.118 for phasor measurement and OPC UA for M2M communication. In many application cases, it's required to map the data from protocols to another. There is a lack of a common data bus or interface that can be used by the application developer to develop smart grid application, such as Energy management systems EMS or demand side management systems.

1.6 Communication challenges

The communication network for smart grid applications should consider the special requirements for real-time control. Smart grid control relies on different types of signals; each type of signal has a special requirement regarding the bandwidth, delay, and availability. The data availability means the ability to access the right data at the right

time. The communication infrastructure design should be coordinated with the control requirement. Some data are sensitive to delay, such as the protection and feedback signal in low inertia systems. The communication middleware is a critical component in smart grid control. The smart grid implementation involves data exchange between local and remote nodes. These nodes represent devices manufactured by different vendors and owned by different entities. The communication middleware provides an abstraction layer to simplify and manage the communication between different nodes without being concerned with the complexity of hardware layers or network details [23][24],[30]. Most of the old protocols use the message-centric approach. The data exchange in the message-centric approach is based on defining a set of messages and data formats to support the expected data types and use scenarios. These messages are predefined and embedded in nodes. Using a set of predefined messages puts some limitations on the system expandability when expansion requires defining new data types or operation scenarios [30].

1.7 Problem statement

The increased penetration of distributed renewable resources located on the distribution side requires extending the current communication infrastructure. This is because the distributed nature of the renewable resources force re-shaping the grid structure from centralized to decentralized control architecture. The decentralized architecture utilizes the microgrid to integrate and manage the distributed energy resources, loads, and provides services to improve the overall system performance. The distributed architecture also requires an extension of the communication network to the

distribution side and integration with several types of software and computational technology. This integration raises challenges related to security, scalability, interoperability, and interaction between the cyber and the physical components.

To address these challenges, the co-design of a scalable communication and control framework taking into account the interoperability, the security issues, and the physical system requirements, is required. A new set of tools that simulate and represent the system as an integrated cyber-physical system to understand the complex system dynamics and test new ideas in a safe and practical environment is also required. Investigating the vulnerability and attack surface of this type of integration is also important in order to provide mitigation mechanisms that take into account the impact on the physical system operation.

1.8 Research Objective

The concept of the co-design of a security-aware power system is presented in this dissertation. The idea of the co-design of the cyber-physical system is to consider the mutual interaction between cyber and physical component from initial design instead of dealing with the design as a separate stacked layer. Detailed analysis of the physical system and control requirement should be taken into account during the design of the communication and cyber layers. On the other side, the impact of the cyber layer should be considered in the design of the physical and control layers. In the security aware system, security is an essential component in the design. Security measures must be taken into account in the design of the component level, as well as system level. Adding the security as an additional layer in the final system design could interfere with the physical

system operation and not be feasible in many cases. Once this co-design is achieved, the proposed design technique will improve the grid resiliency and security. The co-design process deals with the interaction between cyber and physical components. Therefore, a hybrid hardware and software testbed environment is developed to accurately represent the power system as an integrated cyber-physical system. The hybrid modeling environment utilizes the simulation software packages to simulate large-scale systems and capture macroscopic details while benefiting from high-resolution details of the hardware system. Moreover, the testbed environment allows testing developed idea with real hardware and communication network, in addition to protocol emulation and devices virtualization.

The main goal of the co-design is to improve the system performance, reliability and reduce the vulnerability. To achieve this goal, the concept of the co-design is applied to the design of the microgrid synchronization, islanding detection, distributed DC-DC converter control, and energy management system. In addition, security mechanisms that address the cyber security vulnerability in a smart grid standard and customer privacy issues due physical systems' characteristics, such as system current and electromagnetic signatures, are developed.

1.9 Original contribution of this dissertation

The original contribution of this desertion is to develop techniques for co-design of security aware power distribution systems as a cyber-physical system. To achieve this goal, a detailed study of the communication requirements for the smart grid to integrate microgrids and distributed resources in the distribution network is performed. The

purpose of this study is to address the important issues for proper integration of microgrids, such as the real-time control requirements, the need for interoperability, cyber security of the communication infrastructure, and scalability issues. This study resulted in designing and implementing an interoperability and communication framework for microgrid control, taking into account its cyber and physical security. First, the interoperability layer provides a common data bus and a resilient communication and control environment for seamless integration of microgrids. Then, a defined data model for the controllers, sensors, and power system components introduced to enhance the overall system operation and communication resiliency.

In order to improve the current distributed resources, monitoring and management in the distribution network, an advanced metering infrastructure (AMI) was developed and implemented. This AMI includes smart meters, communication network, head-end, and meter data management system, and home area network gateway. The developed infrastructure seamlessly integrated with the developed microgrid communication and control framework. Moreover, a synchronized measurement network was developed and implemented to provide real-time monitoring, as well as situational awareness for the distribution network. This real-time synchronized network provides high-resolution phase angle measurement along with voltage and current measurements. In the developed network, the utilized data-centric communication middleware eliminates the need for using a phasor data concentrator and ensures the delivery of multicast data streams via the reliable real-time publisher-subscribe (RTPS) protocol.

To test and verify the developed algorithms and control frameworks, a hybrid hardware/software testbed environment was developed to represent the microgrid as a cyber-physical system. The developed platform is utilized to perform different types of simulation experiments, such as HIL as well as SIL operational control in real-time. The hardware in the loop platform provides the method of simulating a large power system network while at the same time interacting with actual hardware components. The integration between the proposed co-simulation framework and smart grid testbed will provide a flexible hybrid software/hardware environment for modeling and testing different smart grid operating scenarios. Finally, the proposed framework provides a standard and flexible interface to integrate with other testbed facilities from different domains for multidisciplinary studies. This type of integration provides the scalability to represent large cyber-physical systems.

The work in this dissertation utilizes communication technologies to enhance the performance of the distributed DC –DC converters in the microgrid and DC distribution network. The dissertation extends the application of the GPS synchronization to the DC microgrid. GPS synchronization has been widely used in PMUs for synchronized measurements in the AC networks; however, to the best of the author's knowledge, it has never been used to enhance the power quality in DC networks. The importance of the proposed synchronization method is to allow the operation of distributed DC-DC converters' modulators as an interleaved converters system. The interleaved operation reduces the ripple, and therefore, the DC-link capacitor size. In addition to that, the

synchronization method improves the system electromagnetic compatibility by reducing interferences from the harmonics.

Along with utilizing the GPS signal for distributed DC-DC converter synchronization, a new technique was developed to improve the system's security and reliability. This technique is proposed as a backup for the GPS synchronization in the DC microgrid in the case of GPS signal spoofing, jamming, or blocking. The technique is based on carrier extraction synchronization to maintain the synchronization of the converters without relying on the GPS signal. To achieve that, a real-time phase angle optimization technique to minimize the DC bus voltage ripple in the DC microgrid and DC distribution network is developed.

To address the integration of the microgrid and distributed resources with the utility system, a new synchronization scheme was developed to improve the synchronization accuracy and maintain the stability under distorted voltage waveforms and fault condition. Also, an islanding detection algorithm is implemented to overcome the problem of SCADA and PMU islanding detection methods. To ensure continuity of operation in islanding and grid-connected modes, a reconfigurable controller is developed.

Since the smart grid contains several dispersed microgrids, the work in this dissertation developed a distributed energy management system that includes online optimization and takes into account the privacy and security of customer data. The energy management system represents the application layer on the top of previously developed physical, communication and control layers. The developed application will collect

information from AMI, synchronized measurement network and control power electronics converters, energy storage, and distributed renewable energy source to optimize the energy usage based on the available renewable energy and real-time prices.

Modern communication and signal processing techniques threaten the customer privacy. That is, privacy can be exposed by leaking information from the cyber and the physical components. From the cyber component, information can be leaked through attacking and/or hacking the communication infrastructure. From the physical component, the system's physical characteristics can be used to extract information about the behavior of the customer. The cyber privacy is address by utilizing proper encryption and authentication techniques, whereas two techniques were developed to address the physical privacy issues. The first technique is to hide or change the current signature that can be used to identify the customer load and operation pattern. Second, the electromagnetic signatures, which can be utilized to identify the system remotely, are reduced using the developed online electromagnetic signature monitoring and reduction technique.

Finally, the work in this dissertation focuses on the cybersecurity issues related to industrial standards for power system automation. A detailed security and vulnerability analyses were performed to identify weak points and attack surfaces for the IEC 61850 standard. Based on this study, a security mechanism for IEC 61850 GOOSE messages was developed to address the security shortcomings in the standard.

1.10 Dissertation organization

This dissertation is organized in fourteen chapters, including this chapter, which introduces the general contributions of this dissertation.

Chapter 2 discusses the communication requirement for modern power system and addresses the scalability and interoperability problems related to message-centric approaches by implementing a common data bus based on the data-centric approach; and proposes a hybrid hardware/software infrastructure for microgrid control that seamlessly integrates communication, software, and physical components. The design of the data structure and a standard interface for the developed infrastructure are provided.

Chapter 3 presents the development of an AMI that integrates seamlessly with the microgrid's communication infrastructure presented in Chapter 2. It also discusses the modular architecture, hardware and software details of the developed AMI, which consists of smart meters, a communication interface, and home area network (HAN) gateway modules. These modules are built based on a custom developed firmware that allows real-time monitoring, real-time price exchange and interaction with customer systems through the HAN gateway. This real-time interaction is necessary for the implementation of microgrid energy management systems, demand-side management and distributed renewable energy resource integration.

Chapter 4 extends the hybrid software/hardware infrastructure developed in chapter 2 by proposing a synchronized measurement network for the distribution system. The proposed measurement network supports completely distributed and resilient peer/peer communication environment. The developed measurement unit can directly measure the

phase angle, frequency and the magnitude of the voltage and current fundamental components. The details of the developed hardware and firmware are presented.

Chapter 5 explains the details of the developed hybrid hardware/software-based smart grid testbed infrastructure to represent the interaction of the cyber and physical component of the microgrid. The proposed testbed infrastructure provides the necessary hardware and software environment to perform different types of experiments, such as HIL, as well as SIL operational control in real-time. It also provides an interface to integrate with other testbed facilities from different domains for multidisciplinary studies. The testbed interface enables remote experimental features to perform experiments, test developed algorithms, and collect data remotely.

Chapter 6 introduces the phasor measurement and GPS synchronization to the DC microgrid applications. GPS synchronization has been widely used in the PMUs for synchronized measurements in the AC networks. To the best of the author's knowledge, it has never been used to enhance power quality in DC networks. Introducing the GPS synchronization to the DC networks allows the operation of distributed DC-DC converters modulators as an interleaved converters system. The interleave operation of distributed DC-DC converters reduces the ripple and DC-link capacitor size. In addition, it improves the system electromagnetic compatibility by reducing interferences from harmonics.

In Chapter 7 a new method for synchronizing PWM modulators of distributed DC-DC converters is presented. The proposed synchronization method utilizes a carrier extraction technique to extract the carrier frequency from the DC bus ripple to generate a common

frequency reference. This method provides a backup or alternative synchronization method to prevent degradation of system performance in case of GPS signal jamming, spoofing or blocking. In addition to the carrier extraction synchronization method, a new phase shift control algorithm inspired from carrier sense multiple access communication is developed to optimize the carriers' phase angle. The developed control is completely distributed and doesn't require a communication channel between converters.

Chapter 8 introduces an accurate synchronization technique for the microgrid with distributed energy resources based on the adaptive synchronous reference frame phase locked loop under unbalanced and distorted voltage condition. The developed synchronization algorithm is equipped with an islanding detection algorithm that overcomes the PMU and SCADA system islanding detection problems. In addition to synchronization and islanding detection methods, this chapter introduces a reconfigurable grid tie converter controller. The reconfigurable controller seamlessly switches the converter operating mode from power control mode during grid connection to voltage control mode during islanding. The superior performance and unique features of the developed synchronization, islanding detection, and reconfigurable controller increase the microgrid stability and reliability.

Chapter 9 introduces a complete scalable energy management system framework for a small microgrid or nano grid. The energy management system represents the application layer on the top of previously developed physical, communication and control layers. The developed application will collect information from AMI, synchronized measurement network and control power electronics converters, energy storage and distributed

renewable energy source to optimize the energy usage based on the available renewable energy and real-time prices. This chapter also addresses the privacy and security issue related to the AMI and energy management systems.

Chapter 10 addresses the customer privacy and information leakages from customers' consumption data and current signature. Using this leaked information, a monitoring entity can reveal private customer behavioral patterns, as well as the type of equipment used and or owned. To prevent or minimize the information leakage, this chapter introduces a technique to hide or change the current and consumption signature by utilizing an active power filter.

Chapter 11 discusses the security threat results from radiated electromagnetic signatures.

The electromagnetic signature for high-current devices can be detected and identified remotely. Remote identification of equipment's electromagnetic signature raises privacy and security concern for some types of power systems, such as a shipboard power system. Detection of electromagnetic signature remotely represents a threat to military ships. A new technique to minimize the radiated field from heavy current loads, such as electrical propulsion motor, is developed in this chapter. The developed method can be implemented online without a need to revise the construction of the drive or the machine.

Chapter 12 provides an overview and vulnerability analysis for one of the most accepted standards for data modeling and communication in the modern power system. The IEC 61850 is widely accepted standard in substation automation and microgrid control. The cyber vulnerability related to the IEC 61850 communication protocols and related

security standard IEC 62351, as well as the motivation to develop a new security algorithm for the IEC 61850, is discussed in detail in this chapter.

Chapter 13 focuses on development and implementation of a security mechanism based on the sequence hopping to secure the IEC 61850 event messages. The developed security mechanism provides protection and intrusion detection methods to protect critical substation automation assets from attack while utilizing minimal processing resources.

Chapter 14 provides a summary of the dissertation outcomes, the significance of this research as well as recommendations for future work related to its topic.

Chapter 2 Microgrid Cyber-Physical Infrastructure

2.1 Communication requirements for smart grid

The future utility grid will be characterized by tight integration between power electronics, sensing, protection, control, communications technologies, and DER. Most DER will be installed on the distribution network, which, already in its current state, lacks the proper communication and control network necessary to control the applicable resources [31]. A communication infrastructure needs to be designed to provide a more efficient and flexible way to manage the energy flow keeping interoperability in mind [32][33]. On one hand, this type of integration can dramatically improve the grid performance and efficiency, but on the other, it can also introduce new types of vulnerabilities to the grid [34], complicating the system's analysis and the design process [35]. Ensuring interoperability between different equipment, software packages, and protocols is challenging. Real-time operation and data exchange is another challenge.

The communication middleware is a critical component in a smart grid control. The communication middleware provides an abstraction layer to simplify and manage the communication between different nodes without being concerned with the complexity of hardware layers or network details [36],[37][38] Moreover, the middleware should provide a standard application programming interface (API) to different applications and controllers. Using a standard API reduces the efforts needed to develop new devices and applications for the smart grid. Several types of communication middleware are available and used in different industrial and control applications [33]. The communication middleware can be categorized into message- and data-centric. Traditionally, message-

centric protocols are utilized in utility applications. However, the new data-centric middleware approach has more advantages over the message-centric, as it has more ability to be expanded.

The work presented in this chapter addresses the scalability and interoperability problems related to message-centric approaches by implementing a common data bus based on the data-centric approach; and proposes a hybrid hardware/software infrastructure that seamlessly integrates communication, software, and physical components. The design of the data structure and a standard interface for the developed infrastructure are provided.

2.2 Communication Middleware for Smart Grid Applications

The communication middleware for smart grid applications should consider the special requirements for real-time control. Microgrids and low inertia generator control need low data latency to support fast control actions and maintain stability. The communication middleware should also provide a wide range of quality of service (QoS) profiles to meet the different needs of controllers and data types [33],[37]. For example, the measurement data could be discarded in case of a delay when a new sample becomes available, while the circuit breaker (CB) states should be persistent to ensure its proper operation. Certain types of data are tolerant to delays, such as smart meters and power quality measurements, while other data types, such as data related to protection and fault detection, are sensitive to delay. The middleware should be aware of the data types and its requirements to provide the correct priority for each data type. Communication reliability is essential in real-time applications [37]. Therefore, the middleware

implementation should also avoid a bottleneck and single point of failure in the communication network [39].

The smart grid implementation involves data exchange between local and remote nodes. These nodes represent devices manufactured by different vendors and owned by different entities. The middleware should abstract the complex network details from the user and provide a simple communication interface without dealing with complex details about the network topology and nodal information, such as a location or address [40].

One of the main challenges in the smart grid is the dynamic participation of different devices and systems, ranging from smart appliances to large systems, such as microgrids [33]. The communication middleware should provide a way to handle dynamic participant nodes and an auto discovery features for newly joined nodes. The communication and power network topology should have the capability to be changed under catastrophic or emergency conditions. An auto discovery and dynamic participation feature will support the reconfiguration of a distributed control system. The modern grid is very susceptible for future expansions; thus, the used middleware and communication infrastructure should be capable of handling these new expansions. An expansion process should be done without the need to redesign or modify the implemented protocols. Furthermore, the communication middleware must provide a standard communication interface to ensure interoperability among different vendors and devices. To ensure system operation and reliability, the communication network should be protected by a proper encryption and authentication mechanism. The middleware should provide the security features embedded in the implementation to secure the data

exchange and prevent altering data or violating customer privacy [41]. Since most smart grid controllers and IEDs use low power processors with limited memory and hardware resources, the middleware implementation must support a small footprint for limited resource devices [33].

The communication middleware can be categorized into two main categories: message-centric and data-centric. The differences between both and selection criteria will be discussed in detail in the following subsection.

2.2.1 Messages-Centric Middleware Approach

The data exchange in the message-centric approach is based on defining a set of messages and data formats to support the expected data types and usage scenarios. These messages are predefined and embedded in node applications. In a message-centric approach, the unit of the information is the message; the message can contain different types of information. For example, the IEEE C37.118.2 synchrophasor measurement standard defines four different message types for PMU and phasor data concentrator (PDC), as below:

- Command message

  The command message is sent to the data source (PMU/PDC) for control and configuration.

- Data Frame

  The data frame is sent from a data source (PMU/PDC) to receiving nodes.

  Data frames contain phasor, frequency, analog measurements and digital data types.

- Configuration message

  Configuration message describes the data types, calibration, and meta-data for the data sent by PMU/PDC.

- Header message

  The header message is a readable descriptive text information provided by the user and sent from the PMU or PDC.

The message frame is depicted in Figure 2.1. All message frames consist of SYNC, FRAMESIZE, IDCODE, SOC, FRASEC, and DATA AND CHK fields. The two bytes SYNC field is used to identify the beginning of the new message, designate the frame type and protocol version. The FRAMESIZE field contains the total number of bytes in the frame, including the CHK field. The IDCODE field is the data stream ID which identifies the destination for a command frame and the source for other messages. The time stamp is transmitted in SOC and FRACSEC fields. The SOC field, or second of the century, is a 32-bit integer number representing the time in seconds starting from midnight 01-Jan-1970. The FRACSEC field contains the fraction of second and time quality information. The data field could be an integer or a float data type based on the device configuration. All message frames end with a CHK field, which contains a cyclic redundancy check CRC-CCITT for data integrity.

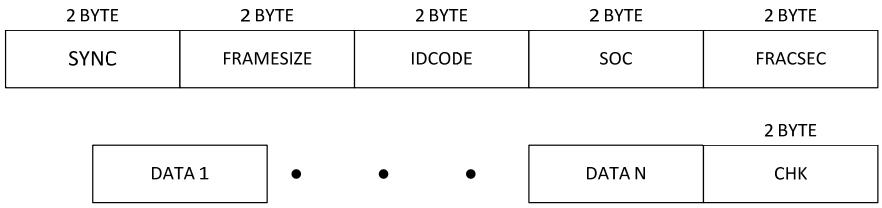


Figure 2.1. C38.118 message frame

The message frames shall be transmitted in their entirety as they are specified by the standard. The message frame can be transmitted over RS232 or Ethernet connection. When frames are transmitted over stacked protocols, such as IP protocols or IEC 61850 manufacturing messaging specification (MMS), the entire frame including SYNC and CRC-CCITT shall be written into and read from the application layer interface. In this approach, the communication infrastructure has no information about message contents or data types, thus the message parsing, data filtering, and integrity check are done on the application level. Each node is responsible for assuring the correctness of the data types it receives according to the configuration and tracks the state of the data of interest locally [42]. Here, any mismatch can cause malfunction of the application. The data field types and meaning depend on the device configuration. The data frame is not enough to correctly interpret the data fields. The application also needs to receive the device configuration.

This approach has several drawbacks. Implementing the message parsing and integrity checks on the application level put more responsibility on the control application developer, which makes the development more complex and time-consuming. Filtering the data of interest at the application layer causes poor network utilization, wasting bandwidth and adding extra processing overhead on the application's processor. The communication infrastructure has no information about the content of the message frame. All fields have to be interpreted by the application. The application needs to receive, parse and validate the whole frame, even if it's interested only in a subset of the data included in the frame.

Using a set of predefined messages puts some limitations on the system expandability when expansion requires defining new data types or operating scenarios [33]. Since the message handling is done at the application level, any change in the message formats or data types requires major changes on the application implementation. Increasing the complexity of the control application by using the message-centric approach can increase the chance of software bugs and decrease the overall system reliability. The vendor-dependent implementation of message parsing and handling algorithms could lead to a wide range of different vulnerabilities, adding more complexity for system maintenance [42],[43].

2.2.2 Data-Centric Middleware Approach

In the Data-Centric approach, the application is developed to deal with the data types of interest only without any concern with the message structure or network details. The message is built by the communication middleware to update a change in the system state [44]. The fundamental unit in the data-centric communication is the data object. The message structure is derived directly from the system data model. Since the message is created by the middleware, the communication infrastructure will be aware of the message contents and data types. The data-centric infrastructure does all the message parsing, data filtering, and integrity checks on the middleware level to ensure the delivery of correct data types and the system state to all nodes.

This approach offers more capabilities over a traditional message-centric approach. Moving the message processing responsibility from the application to middleware not only simplifies the application development but also increases the system reliability by

reducing the number of errors that results from different implementations of message parsing. Implementing the data filtering on the middleware layer could result in a more optimum utilization of the network bandwidth [42]. The infrastructure awareness of the data types makes it possible to assign different QoS profiles, priorities, and security levels based on the data types instead of the message types, as is the case in the message-centric approach.

Since the middleware is responsible for all message processing tasks and the applications are concerned only with the data object, adding new data types will not require modification of existing applications. This feature is essential for an expandable system, such as the continuously evolving smart grid. Figure 2.2 depicts both middleware approaches, where message-centric is on the left and data-centric on the right.

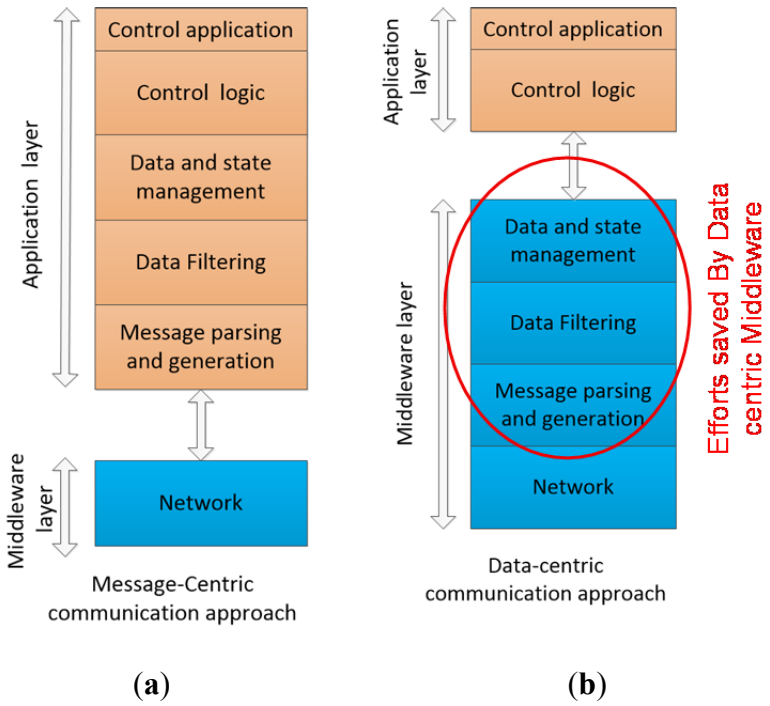


Figure 2.2. Middleware approaches: (a) message-centric; and (b) data-centric adapted from [54]

Throughout this dissertation, the proposed communication framework utilizes data distribution service (DDS) standard for the communication middleware. The DDS is a standard for data-centric communication from the Object Management Group (OMG). The DDS has unique features which improve the smart grid communication drastically, as described below:

- DDS moves the message construction, message parsing, data filtering, and validation from the application to the middleware layer. Moving the message construction process from the application to middleware layer improves the system scalability and enables adding new types of data for new operation scenarios without the need to modify existing applications.
- DDS utilizes real-time publisher-subscriber protocol, which enables peer-to-peer communication without a message broker. This communication scheme improves the smart grid reliability by avoiding a single point of failure. Publisher-subscriber and peer-to-peer communication provide a more suitable environment for distributed controllers.
- DDS supports automatic discovery of newly-joined devices and their data structures. This feature allows dynamic participation of network nodes, which are important, especially for microgrids, where different nodes can join and leave the microgrid network, such as electric vehicles and smart devices.
- Unlike other communication methods that apply quality of service profiles for a whole data stream or protocols, DDS can apply different QoS for each data type,

which provides a more flexible communication management and leads to a more predictable behavior. QoS profiles give the ability to define the allowed latency budget, data durability for late joining devices, and data lifespan. More descriptions of QoS and its synergy to the power application will be provided in the next section.

2.3 Data Distribution Service Infrastructure for Smart Grid Testbed

The communication network infrastructure for the smart grid should provide a flexible and scalable environment to connect different system components and exchange information in real-time. There are different types of communication networks. One of these types is client-server network communication. In this type, the communication is centrally managed by the server. This central management represents a single point of failure and a bottleneck, which could affect the reliability of the network. While in point-to-point communication, the communication is established directly between the nodes without a message broker, which is hard to manage in large networks [39]. To meet the hard real-time requirement and scalability of the smart grid, the DDS middleware is chosen for the communication network. The DDS utilizes publisher-subscriber without a message broker scheme which simplifies the communication between different nodes [45][46],[47]. Furthermore, the DDS is data-centric middleware, which helps to maintain the focus on the data model, algorithm and control development rather than being concerned with communication and data delivery issues [44][46]. The data-centric approach also allows assigning different QoS profiles to an individual data type instead of the whole stream.

2.3.1 System interoperability

Highly motivated by its high reliability and unique features, the DDS found its way to being used in a wide variety of mission-critical applications. For example, DDS is implemented by the US Navy and Lockheed Martin in radar and ship management systems [48]. Furthermore, DDS has been adopted in Air Traffic Control centers in some European countries [49], large financial firms, automation and SCADA systems for large projects, including Grand Coulee dam in Washington State (USA) [50], and automotive applications. The DDS is selected by the smart grid interoperability panel (SGIP) and Duke Energy for Open field message bus (OpenFMB) implementation to create a distributed, intelligent platform that supports publisher-subscriber messaging [51].

The real-time publisher-subscriber wire protocol ensures the interoperability [52], real-time performance and automatic discovery of new services. Moreover, the publisher-subscriber protocol is utilized by the IEC 61850 protocol and has started to gain more popularity in IEDs [37]. The DDS has an advantage of covering a wide range of applications, ranging from non-real-time to extreme real-time application. Figure 2.3 shows a comparison between DDS, Common Object Request Broker Architecture (CORBA), Real-time CORBA (RT-CORBA) Java messaging system (JMS), the Real-Time specification for Java (RTSJ) and message parsing interface (MPI). The comparison is based on an analysis done by Naval Surface Warfare Center NSWC [53].

The standard API for the DDS middleware provides the necessary tools to integrate with different simulation and analysis software with support for several programming languages, such as C, C++, and JAVA. The DDS also supports Java Messaging System

JMS, which enables integration with JAVA-based multi-agent platform, such as Java Agent Development Framework (JADE). Since DDS standard focus on the data model instead of messages, standard data model, such as IEC 61850 and IEC 61970-301 common information Model (CIM), can be mapped to DDS.

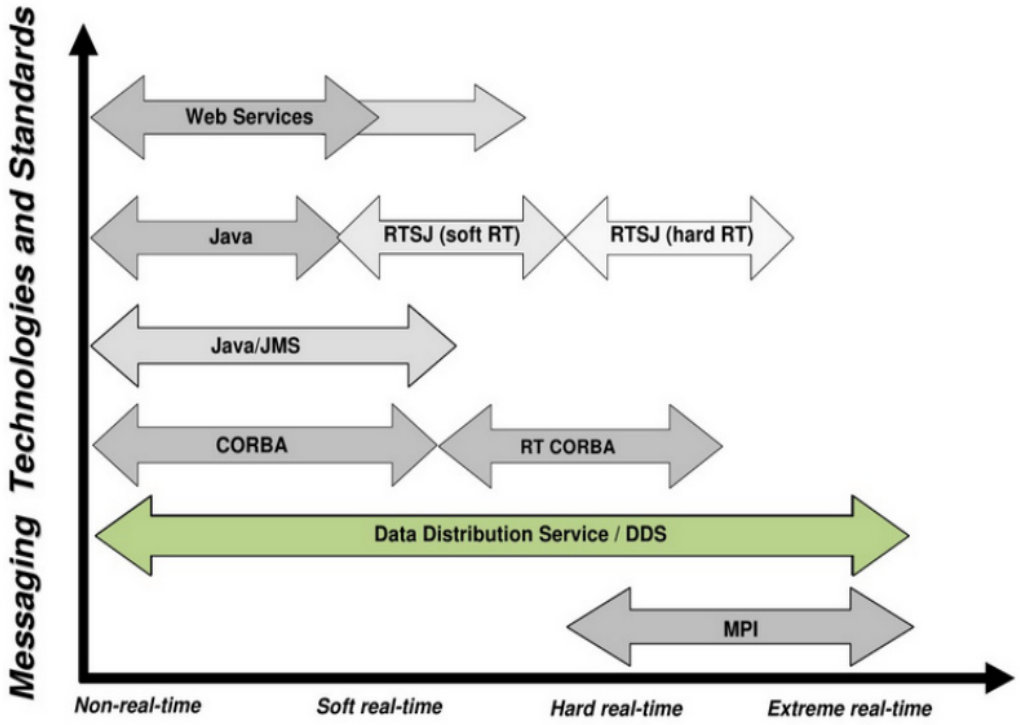


Figure 2.3. DDS applications vs different communication standard

Although other middleware services exist, DDS provide the most reliable interoperability solution compared. One popular middleware service is OPC or OLE for Process Control. OPC is a platform independent standard through which various kinds of systems exchange messages based on a client-server approach, unlike DDS, which follows a publish-subscribe method. It was introduced as a means to shield client applications from the details of the automation equipment and providing standardized interfaces to interact with control hardware and field devices. Applications developed on

an OPC middleware interact by invoking requests on UA servers, which make them suffer from a single point of failure (i.e. the server), as shown in figure 2.4. However, in DDS, applications interact asynchronously and anonymously by reading and/or writing to a global data space.

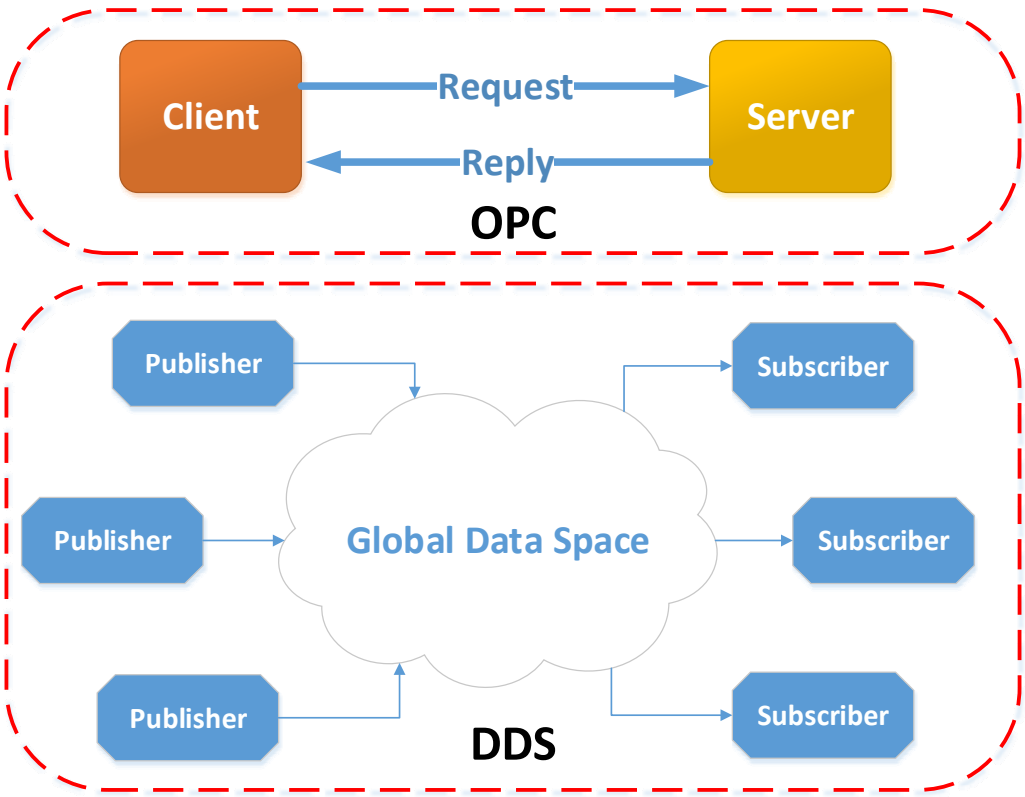


Figure 2.4. DDS vs OPC middleware

Also, a major drawback of OPC is that, unlike DDS, it does not support QoS specification and therefore lacks message prioritization which is important in microgrid applications.

Based on the data-centric approach, implementing the DDS needs to define a data model for the system. This data model defines the structure of the data and its relation

amongst physical hardware objects. For experimentation and verification, a data model is created for a scaled power system in the smart grid testbed at Florida International University's Energy Systems Research lab. The physical hardware description of the scaled power system and the data model are described in the next section

2.4 Physical Setup Description and Data Model

In this section, the physical infrastructure for the smart grid testbed will be discussed. This testbed represents a hybrid AC/DC power system involving distributed architectures and multiple microgrids. The architecture of the network emulates a real power system with microgrids attached to it, utilizing commercial and special purpose power system components.

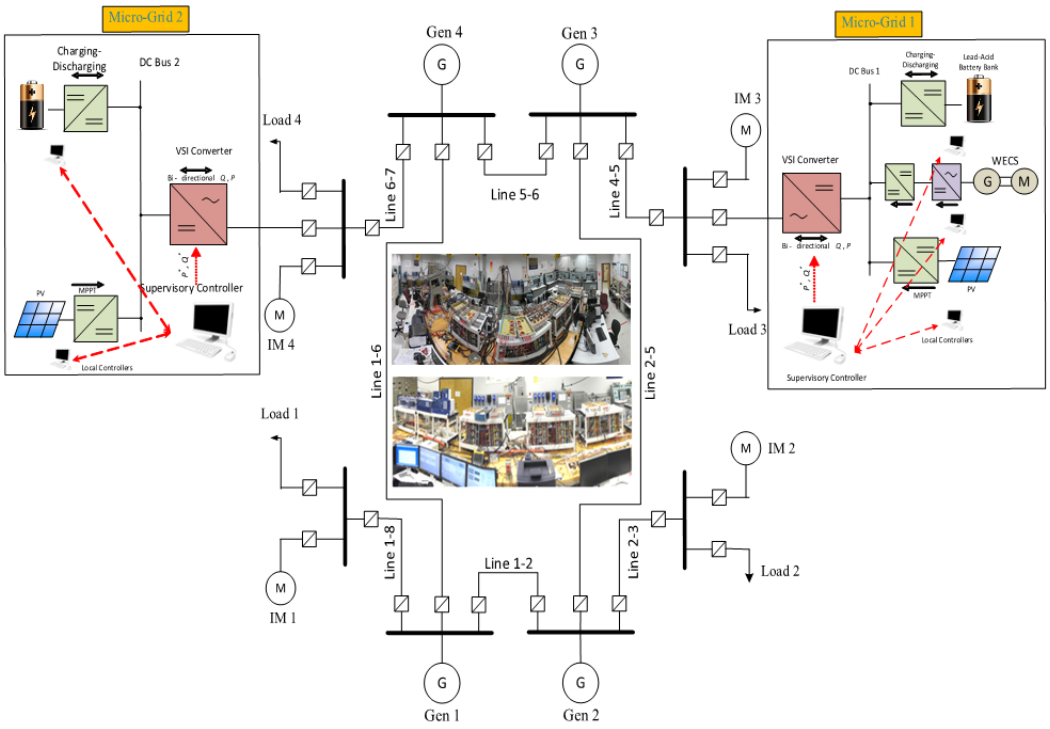


Figure 2.5. Schematic diagram for the smart grid testbed

The microgrids can be used to emulate buildings, commercial facilities or residential communities. The testbed system is scaled down in terms of power and operating voltage to enable its utilization in a laboratory environment [54]. Figure 2.5 shows the architecture of the smart grid testbed implemented at Florida International University (FIU).

2.4.1 Main Grid

The main AC grid consists of four self-excited AC synchronous generators, two of which are rated at 13.8 KVA, while the other two are rated at 10.4 KVA. These generators are driven by different types of motors acting as prime movers. The generators are rated at three phase 208 V, 60 Hz, and 1800 RPM. Each generator is connected through an automatic synchronizer to its corresponding switching and measurement bus. The connectivity of the AC network is realized using various π-section transmission line/cable emulators. A total of 18 transmission line/cable emulators and 14 buses were used. The bus and line modules are flexible to vary system network architectures. The user has full control of transmission line connectivity, system frequency, and the generator operation modes.

2.4.2 DC Microgrids

Two DC microgrids, namely *MG1* and *MG2*, were connected to the main AC grid. The first DC microgrid (*MG1*) includes a photovoltaic (PV) emulator, a wind energy conversion system (WECS) emulator and battery storage. The PV emulator is connected to the DC bus through a DC-DC converter. The WECS is cascaded by an uncontrolled

rectifier followed by a controlled DC-DC converter [55]. The DC bus voltage is 380 VDC.

The second DC microgrid (*MG2*) includes a 6 kW PV and a 6 kW fuel cell (FC) emulators. The system includes a 12 kWh backup lead acid battery array that can support loads deficiencies. A 325 V DC bus is used to integrate the PV, FC, and battery energy to the system. Controlled DC-DC boost converters are used as power conditioning units between each of these sources and the DC bus. A 4 kW space vector pulse width modulation (SVPWM) fully controlled bi-directional AC-DC/DC-AC converter was used to tie each DC network to the AC grid. A power electronics converter is used to control active and reactive power flow between AC and DC grids. The converter is also responsible for voltage regulation on the DC side in grid connected mode, while in islanded mode, the local controller switches the voltage regulation to one of the DC-DC converters interfaced with the PV system. This voltage source inverter (VSI) has the capability of receiving reference values for active as well as reactive power and, hence, will play a major role in the active/reactive power compensation processes.

2.4.2 System Data Model

In order to build a data model for the smart grid testbed, a data structure was defined for each object. The structure for each object defines the object type and related data. Each object has a unique descriptive name and several topics defining the data related to this object. For example, the data structure for the generators is shown in Figure 2.6 The structure name represents the object name and each variable represents one of the object parameters that can be read or modified by the other object. Table 2.2-1 shows a list of

objects and related topics. As shown in Table 2.2-1, each row represents a system object and its related topics. For example, the first row depicts the generator data. G_x is the object type, where x is the generator ID. In the second column, the related topics are defined: *I*a, *I*b, *I*c are the three-phase currents, *V*a, *V*b, *V*c are the three-phase voltages, *f* is the frequency, (*P, Q*) are the active and reactive power, and *sync* is the synchronization signal. In the microgrid case, the object type is MG_x and similar topics, such as the ones in the G-x, are defined, except the topic "*mode*". This topic controls the microgrid operation mode in either islanded- or grid-connected operation. For the smart meter object SM_x, the *PA,* and *QA* topics represent the accumulated active and reactive energy, respectively. For the PV emulator PV_Em_x, *I*r, and *T*emp topics represent the solar irradiance and temperature, respectively. *W*s is the wind speed for the wind turbine emulator object. Figure 2.7 shows the DDS infrastructure for the smart grid testbed. The measurements from data acquisition (DAQ) and smart meters were collected and published to a global data space. The DDS DAQ and controller are implemented on an embedded board based on the Sitara AM35xx chip from TI, which provides a high-performance 32-bit 1 GHz ARM processor and two slave 32-bit 200 MHz programmable real-time units (PRU) on-chip. The main processor is utilized to run the operating system and manage the communication. The PRU are utilized to handle hard real-time, fast IO operation, DAQ, and data pre-processing. Linux, with a real-time kernel, is chosen as the operating system to manage hardware resources and provide the TCP/IP stack. For DDS implementation, an open source library provided by real-time innovation (RTI) is used and compiled to work on the embedded ARM board. The DDS library provides the API for Java and C++.

Table 2.2-1. Objects and topics list. Photovoltaic: PV

Object Type	**Topics**	**Description**
G_x	*I*a, *I*b, *I*c, *V*a, *V*b, *V*c, *f*, *P*, *Q*, sync, status.	Generator where x is the generator index.
CB_x	Status	Circuit breaker (CB) where x is the index.
L_x	*P*, *Q*.	Load where x is the load index
Bus_x	*V*a, *V*b, *V*c	Bus where x is the bus index
TL_x	*I*a, *I*b, *I*c	Transmission line where x is the index.
MG_x	*I*a, *I*b, *I*c, *V*a, *V*b, *V*c, *f*, *P*, *Q*, *V*dc, *I*dc, mode.	Microgrid where x in an index.
SM_x	*I*a, *I*b, *I*c, *V*a, *V*b, *V*c, PA, QA.	Smart meter where x is an index.
PV_EM_x	*I*r, *T*emp, *P*, *V*, *I*.	PV emulator with index x.
W_EM_x	*W*s, *I*a, *I*b, *I*c, *V*a, *V*b, *V*c, *f*, *P*, *Q*.	Wind emulator x

For this application, the C++ API was chosen to achieve maximum performance and avoid using a virtual machine. The acquired measurements collected from analog to digital converters or digital inputs are published to the DDS global data space to be made available to all applications. The data subscriber receives the control command/references and digital output status and forwards it to the controllers. The protocol translator, shown in Figure 2.8, is developed to provide an interoperability layer between the DDS and generator speed controllers. These speed controllers are controlled via RS-232 or RS-485. Similar translators can be used for other devices, such as programmable power supplies or load emulators. The controllers and applications can subscribe to receive measurement data or publish control commands for load emulators, generation control, or CBs. As shown in Figure 2.7, the DDS will serve as a common data bus that connects all the system devices and applications.

After defining the data model for the smart grid testbed, it is very important to define the QoS that will be used by the infrastructure to exchange the data. Since the DDS is a content-aware middleware, it allows attaching different QoS policies for each data type and treats each type in a different way instead of applying the same policy on the whole data stream. The user can create custom QoS profiles to control the data exchange for each application. This feature helps to achieve a predictable network behavior with a large number of nodes and different communication requirements [44][56]. The QoS policy defines a different set of rules that controls how the data will be sent and handled by the infrastructure. This set of rules is defined below:

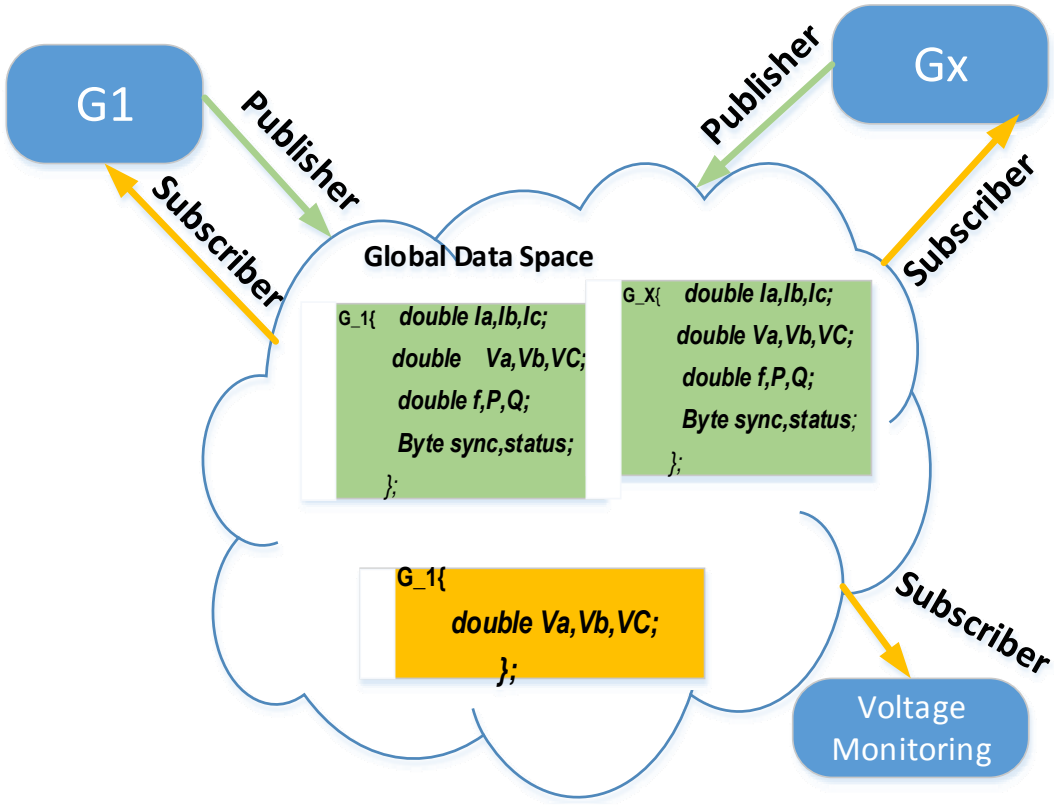


Figure 2.6. Generators data structure and pub/sub example

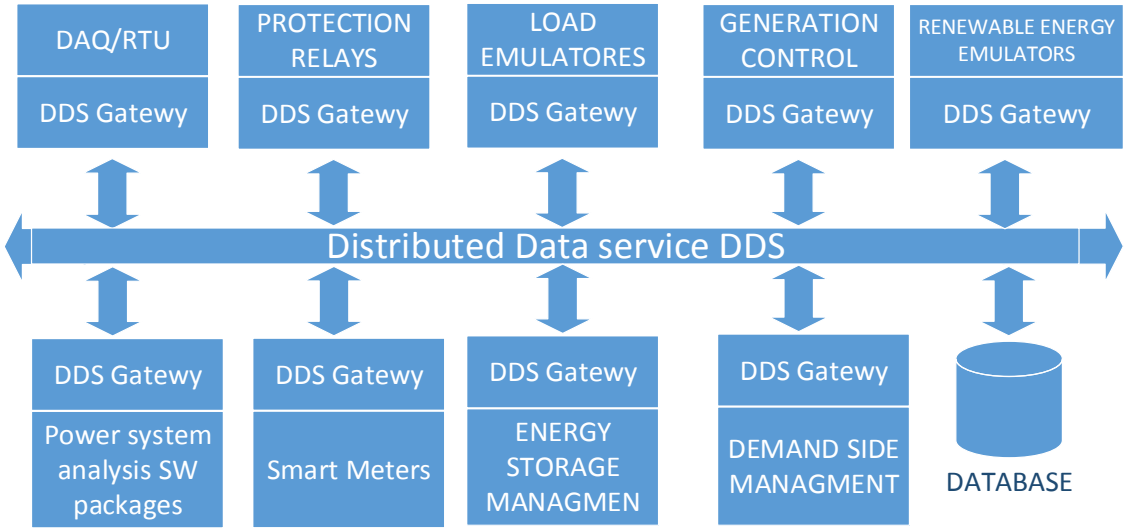


Figure 2.7. DDS testbed infrastructure.

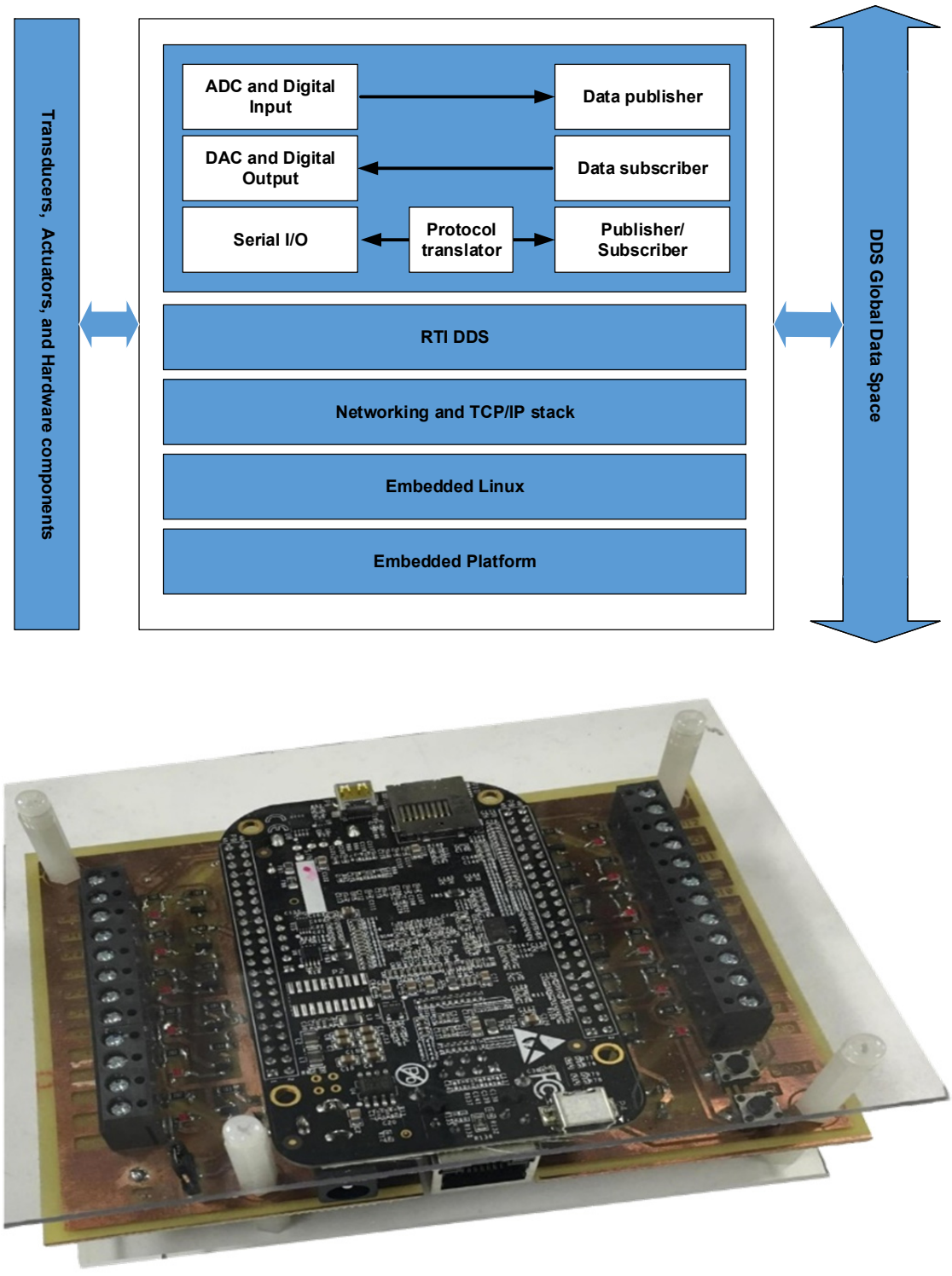


Figure 2.8. The developed data distribution service (DDS) data acquisition (DAQ) and controller block diagram

- Data Availability

The data availability rule controls the availability of the data for a recently-joined subscriber. This rule can be set to a volatile or a non-volatile option. If the data availability is set to volatile, when any publisher publishes or updates any data, all current subscribers will receive the updated data at the instance of an update. Any subscriber, who joins the network after the update instance will not be able to receive the last update. This option is suitable for periodically changing data, such as voltage and current measurements, where the data are updated frequently and old data loses its importance after a short period of time.

The non-volatile data option forces the DDS infrastructure to make the data available for a recently-joined subscriber by storing a local copy of the data. This option is necessary for certain types of data that represent the system state and topology (e.g., CB status, generator running state, *etc.*). This type of information is not updated frequently and will not lose its importance over time. Late-joined nodes must be able to get this type of information when they join the network at any time. The length of the old data that will be made available can also be controlled by the history option. Some applications could function better if they receive longer historical data, such as energy management systems (EMS) that consider the load pattern and utilize prediction algorithms. For this type of application, the DDS can keep longer historical data. For example, late-joined EMS should be able to receive the power consumption measures for the past 24 h. The data availability QoS can be configured by setting the durability and history fields in the

XML file. The durability can be set to volatile, transient or persistence. If the transient option is set, history data will be available for the late joining subscriber. Transient durability will allow the late subscribers to receive the history data as long as the data writer still exists in the network. If the persistence option is chosen, an external persistence service will be used to record the history data and deliver it to the subscriber. Late-joined subscribers will be able to receive history data even after disconnection of the data writer or after a complete system restart. This option is important to restore critical system status after a device failure. The code below shows the XML configuration for Transient durability and a history length of 24 samples.

```
<durability>
<kind>TRANSIENT_DURABILITY_QOS</kind>
<direct_communication>true</direct_communication>
</durability>
<history>
<kind>KEEP_LAST_HISTORY_QOS</kind>
<depth>24</depth>
</history>
```

- Lifespan

The lifespan rule defines how long old data will be valid. The infrastructure will remove the old non-volatile data that exceed the defined Lifespan. This QoS rule ensures

that the control application will not interact based on old invalid data. The XML configuration below is used to set the lifespan for the smart meter data to 24 hours.

```
<lifespan>
<duration>
<sec>86400</sec>
<nanosec>0</nanosec>
</duration>
</lifespan>
```

- Latency Budget

This rule allows defining the priority of the latency sensitive data, such as real-time measurement and protection data. The data with a low latency budget will be sent ahead of the data with a higher latency budget. The protection-related data are always set with the lowest latency budget. Smart meter measurements, price signals, and environment data, such as irradiance and wind speed, are set to the highest latency budget. The XML configuration below is used to configure the lowest possible latency for real-time measurement and protection data by setting the latency budget to zero.

```
<latency_budget>
<duration>
<sec>DURATION_ZERO_SEC</sec>
```

<nanosec>DURATION_ZERO_NSEC</nanosec>

</duration>

</latency_budget>

- Reliability

The reliability QoS rule allows the operator to control how the infrastructure will deal with samples that were not successfully received. The reliability level can be configuring to reliable or best effort. If the reliable option is set, the middleware turns on the RTPS reliability protocol. The RTPS will attempt to repair samples that were not successfully received. If the reliability level is set to best effort, the middleware will not monitor or guarantee that the data is received by the data reader. The best effort reliability level is good for some application, such as data visualization, for other critical data reliable, QoS profile is used. The below XML code set the reliability level to reliable.

<reliability>

<kind>RELIABLE_RELIABILITY_QOS</kind>

</reliability>

- Multicast/Unicast

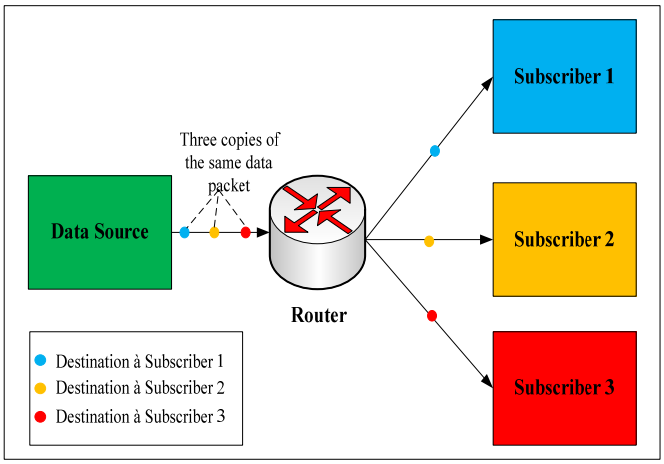
In the unicast communication, the publisher sends a copy of the data for each subscriber node, as shown in Figure 2.9a. For example, EMS and demand-side management systems can subscribe to receive the price and consumption data published by a smart meter. In this case, two copies of the same data will be sent over the

network [37]. If a smart appliance subscribes to the same data, a third copy will be sent to the new subscriber. The bandwidth used to send the data will increase linearly as the number of the nodes subscribing to the data increases. This method of communication could be suitable for local high-speed networks and it is simple to configure, but it is not the ideal method when considering transmitting data over the wide area network (WAN) or a low-speed communication line in the case of wide area measurements and PMU data. For the data requested by multiple readers, it is better to use a multicast communication scheme. In the multicast, the publisher sends only one copy of the data for the remote subscriber, as shown in Figure 2.9b. The bandwidth is independent on the number of subscriber nodes. Only one copy will be sent over the WAN communication line. At the receiving end, the router will forward a copy of the data to each subscriber. In order to use the multicast communication scheme for certain data, a multicast QoS policy has to be applied to this data. For automatic transport multicast mapping, the reader QoS profile is configured, as below.

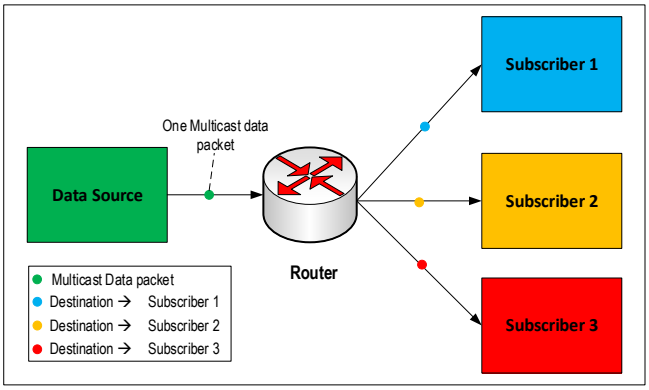
```
<multicast><kind>AUTOMATIC_TRANSPORT_MULTICAST_QOS</kind>
 <value>
 <element>
 <receive_port>0</receive_port>
 <receive_address></receive_address>
 </element>
```

</value>

</multicast>



(a)



(b)

Figure 2.9. (a) Unicast communication; and (b) multicast communication

RTI DDS has additional features that address the challenges of low or limited bandwidth and high latency networks. DDS supports transport priority which enables the control of priority bandwidth utilization [57]. The RTI DDS allows the application to control the traffic load by limiting the maximum throughput and peak bursts [57]. The DDS also gives the application full control over the real-time scheduling policy. DDS

supports three different types of scheduling policies: round-robin (RR), earliest deadline first (EDF), and highest priority first (HPF). The RR scheduling distributes the tokens uniformly across all non-empty destination queues.

In EDF, scheduling the sample deadline is determined by the latency budget and the time it was written. The priorities are determined by the earliest deadline across all samples. The EDF distributes the token to destination queues in the order of their deadline priorities. If two samples have the same priority, the corresponding queues will be served in an RR fashion. In HPF, scheduling the queues is served based on the publication priority. If two samples have equal priorities, the queues will be served in an RR fashion. The EDF scheduler is selected to meet the smart grid real-time application needs since it can dynamically assign priorities to transmitted samples based on its latency budget and deadline. In this way, the scheduler will always give the highest priority to the sample closest to the deadline to avoid violating the latency budget. The critical data will gain a high priority by assigning a low latency budget. Table 2.2-2 shows a summary of QoS profiles for different data type based on the operation requirement. For device status data, such as circuit breaker status, generator availability, and system topology, the status must be available for all controllers and application at any time. To avoid retransmission of the status of the device, the lifespan is set to infinite. The history depth is set to keep the last status. The reliability option is configured as a reliable link to grantee the delivery of status to all subscribers. The latency budget is set to 10ms, this exceeds the highest update rate for PMU. For metering data, a lifespan of 24h and 24 samples are selected to provide current and historical data for energy

management systems. The latency budget for smart meter data is relaxed to 100ms since it's not sensitive to delay.

Table 2.2-2. Quality of Service

Signal	Durability	Lifespan	History (samples)	Latency Budget	Reliability	Unicast/ Multicast
Device status	Transient	inf	1	10ms	Reliable	Multicast
Metering	Transient	24h	24	100ms	Reliable	Multicast
Control	Transient	inf	1	1ms	Reliable	Unicast
Protection	Transient	inf	1	0	Reliable	Unicast
Periodic Measurement	Transient	inf	1	1ms	Reliable	Multicast
Visualization data	Transient	100ms	1	100ms	Best effort	Multicast

System status and smart meter data usually are received by multiple applications, to reduce the bandwidth, multicast transmission is chosen for both types of data. Multicast also reduces the processor overhead on the publisher processor by reducing the number of data streams managed by the processor.

The control signal usually targets a specific device, unicast transmission with reliable transmission protocol is used to transmit the control signal with latency budget 1ms, IEC 61850 allows 3ms delay in critical events. For protection data, the latency budget is set to zero to give the highest priority for protection data over all other types. Reliable QoS is used to grantee delivery of protection data. Periodic measurement has the same QoS profile as control data, except unicast. Periodic measurement uses multicast to allow feeding the data to multiple controllers with reduced bandwidth. Data used in visualization is not sensitive to packet loss since human eyes have a limited ability to detect dropped image frame. Best effort QoS with latency budget 100ms is used for this type of data.

2.5 Network Performance

Real-time control and monitoring require predictive behavior from the communication network. The communication latency and maximum throughput should be known for different scenarios. The message size and data rates are dependent on the application and the data type. Measurements and control commands usually use a small message size, whereas data logging may use a longer message size. Other applications, such as database replications and data backups, will use a long message size. A performance test for the communication infrastructure was performed to benchmark the network performance and

find out the latency corresponding to different message rates and sizes. The performance test was executed by transmitting 10,000 messages and measuring the latency for each message. The test is repeated for unicast and multicast transmission with the best effort and reliable QoS. By knowing the data rate and message size required by the specific application, the users can find out the latency budget and make sure it does not violate the application requirement. Figure 2.10a shows the performance results for the network with unicast. The horizontal axis represents the message size in bytes while the vertical axis represents the latency in microseconds. The test was repeated for different message rates, starting from 50 Msg/s to 1000 Msg/s.

For a message size of 32 bytes, which is more common for measurements and a message rate of 1000 Msg/s, the average latency was 243 μs with 90% below 269 μs and a maximum latency of 336 μs. The performance of unicast transmission with reliable, QoS is shown in Figure 2.10b. The average latency with reliable protocol was 292 μs with 90% below 435 μs and a maximum latency of 727 μs for the same message size and update rate. Figure 2.11 shows the performance test for multicast communication. The performance of best effort is shown in Figure 2.11a. For a message size of 32 bytes with a message rate of 1000 Msg/s, the average latency was 270 μs, with 90% below 306 μs and maximum latency 385 μs. The performance of multicast and reliable quality of service is depicted in Figure 2.11b. The average latency was 255 μs, with maximum delay 534 μs. The performance results are summarized in Table 2.2-3.

When the DDS uses IP-multicast and a node needs to join the multicast group, the node first sends an internet group management protocol (IGMP) join message to the

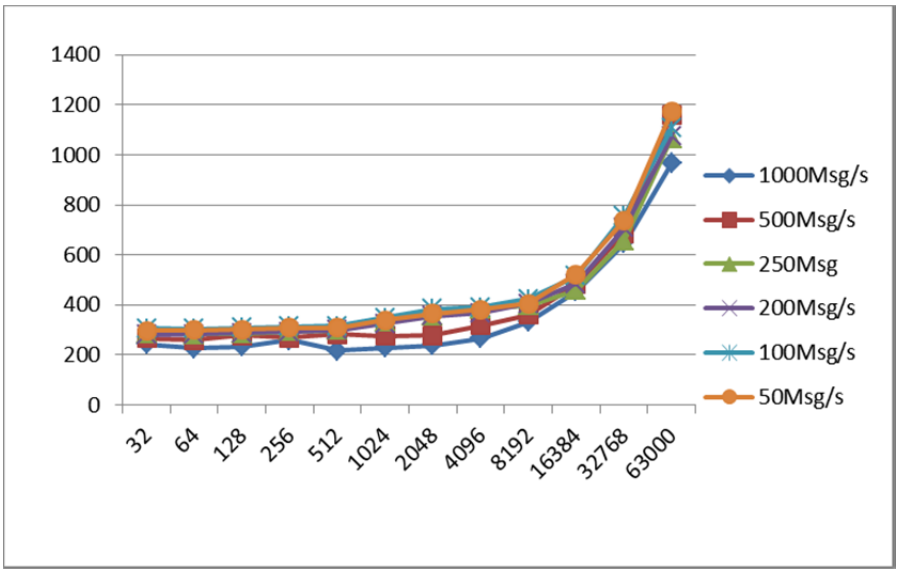
multicast router. Once the node is joined to the multicast group, the multicast router sends an IGMP Query message at a regular interval and waits for an IGMP membership report to confirm the node is still connected to the multicast group. The layer-2 network switch with IGMP snooping enabled creates a list of ports with nodes interested in joining the multicast group.

Table 2.2-3. DDS performance for 32 bytes messages size

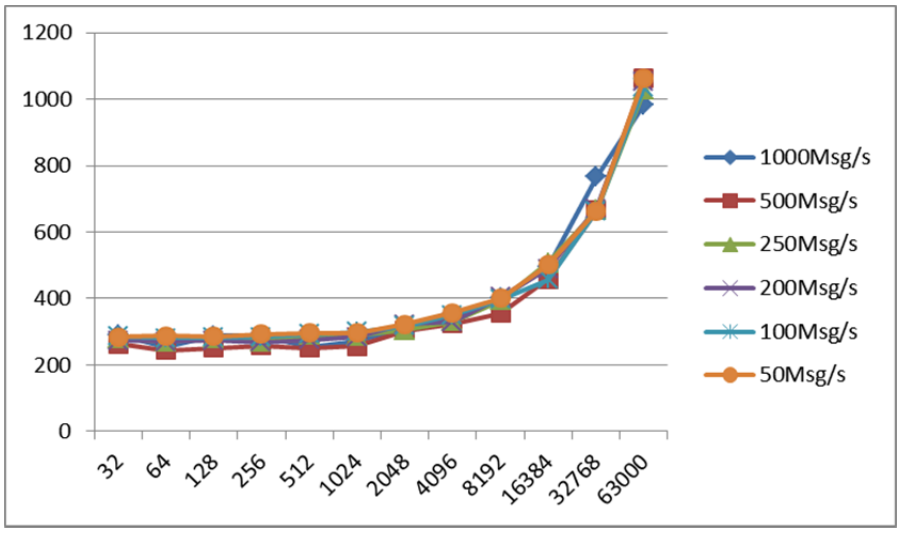
Unicast/Multicast	QoS	Average latency (µs)	Max latency (µs)	90%< t (µs)
Unicast	Best effort	243	336	269
Unicast	Reliable	292	727	435
Multicast	Best effort	270	385	306
Multicast	Reliable	255	534	278

When a multicast message is sent, the switch replicates the data to all ports in the list. The process of multicast and data replication may introduce slightly higher latency compared to unicast. However, multicast is still better than unicast for data requested by multiple nodes and transmitted over limited bandwidth links. Multicast can dramatically reduce the bandwidth required for the data transmission, as compared to the unicast method. The performance test shows that the implemented communication infrastructure has a high update rate and low latency. The obtained update rate and latency are suitable for smart grid real-time applications. For example, PMUs have update rates of 30–60 Msg/s, while IEC 61850 substation automation standard has a restriction of maximum 3

ms delay on critical messages, such as Generic Object Oriented Substation Event (GOOSE), where the benchmarks show that the DDS can achieve 1000 Msg/s with a maximum 0.72 ms.

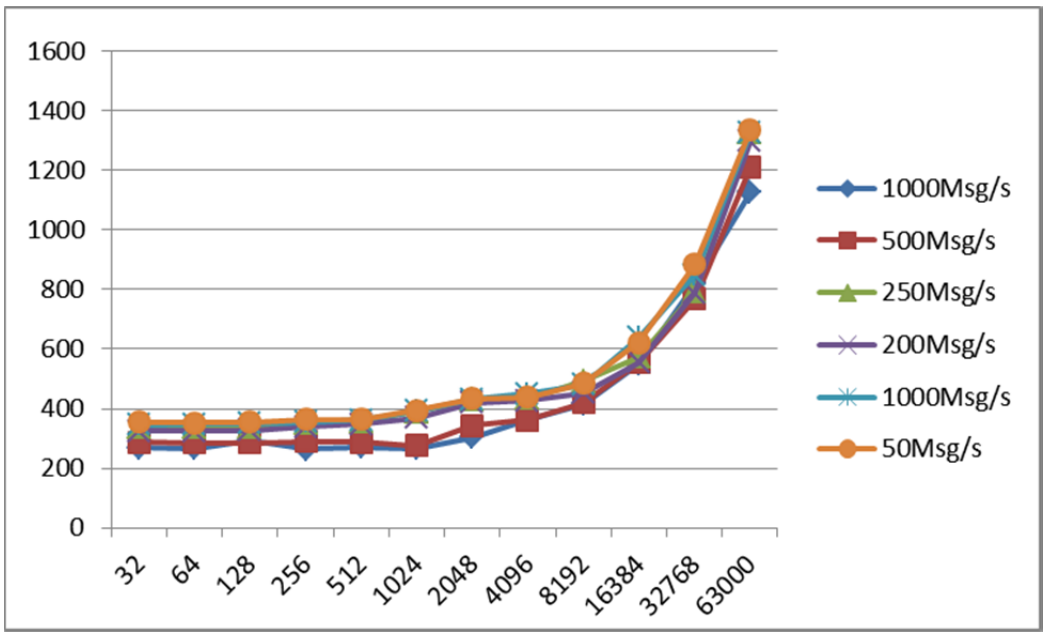


(**a**)

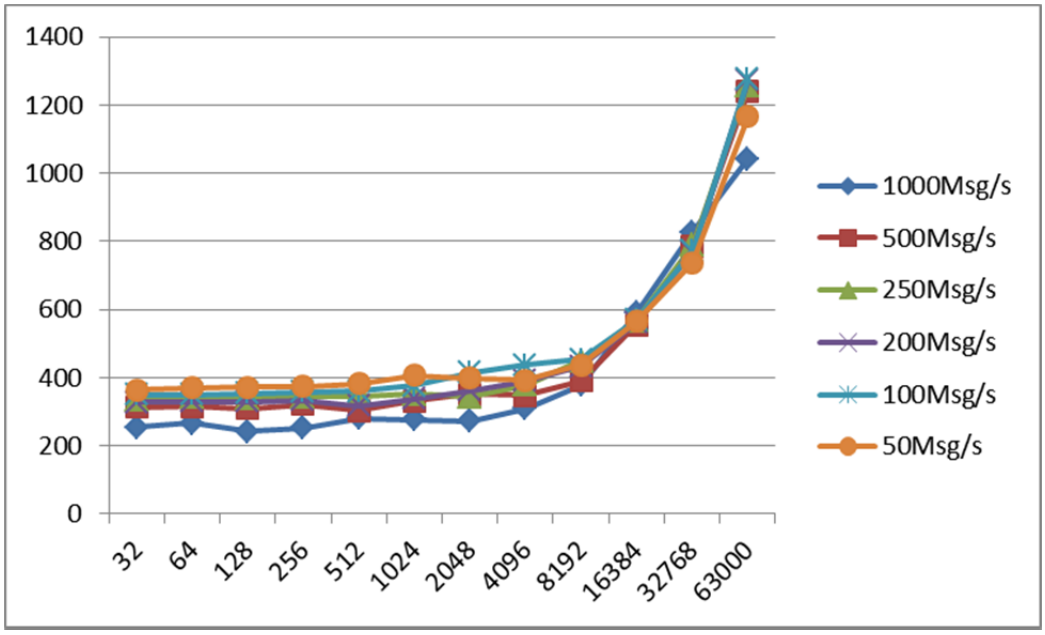


(**b**)

Figure 2.10. a-Performance test for DDS unicast and best effort quality of service b-Performance test for DDS unicast and reliable quality of service (QoS)



(**a**)



(**b**)

Figure 2.11. a- Performance test for DDS multicast and best effort QoS. B- Performance test for DDS multicast and reliable QoS

2.6 Summary

In this chapter, the need for an efficient, scalable and interoperable communication infrastructure for the smart grid has been discussed. To address these issues, this chapter proposed the use of a communication middleware service to manage the energy in the smart grid, keeping interoperability in mind. This is due to the fact that a communication middleware provides an abstraction layer to simplify and manage the communication between different nodes without being concerned with the complexity of hardware layers and network details.

Here, message-centric and data-centric communication paradigms were analyzed. A comparison between both approaches showed that message-centric communications are not easily expandable, as required by the dynamic nature of the smart grid and suffer from a single point of failure. However, in data-centric communications, the fundamental unit is the data object. The message in this approach is created by the middleware, therefore, the communication infrastructure will be aware of the message contents and data types.

As such, the data-centric Data Distribution Service middleware was implemented as a communication backbone for the smart grid test bed. The physical setup and the data requirement for each controller, along with explaining the different QoS profiles supported by the DDS, were presented in this chapter. The design of the data structure and a standard interface for the developed infrastructure were also provided.

Finally, a performance test for the communication infrastructure was performed to benchmark the network performance and find out the latency corresponding to different

message rates and sizes. By knowing the data rate and message size required by the specific application, the users can find out the latency budget and make sure it does not violate the application requirement.

Chapter 3 Advanced metering infrastructure AMI

3.1 Introduction

Advanced metering infrastructure AMI enables two-way communications between end-customers and the utility Company. The goals from this infrastructure are to improve the energy management, detect power outage, enable remote load disconnection and reduce the operation cost by transmitting accurate real-time consumptions data to the utility, which can be extended down to each smart appliance.

In the other direction, the AMI enables real-time energy pricing, which can be used for peak load shaving. The price information and control command can be transmitted to customer appliances and energy management systems EMS through the HAN Gateway. The customer EMS can utilize this information for managing local loads, energy resources and storage to reduce the consumption cost. However, the capabilities of this infrastructure haven't been utilized in most cases due to:

1- Privacy concern.
   Many customers are worried about their privacy and the information that can be extracted from detailed daily usages of their smart appliances.

2- Security Risk.
   To take advantage of the HAN and interaction with a smart meter, strong security rules must be applied to prevent hackers from attacking such systems and control the customer appliance or sent wrong information.

3- Integration with the existing appliance.
   Most of the existing appliances lack a suitable interface to communicate with HAN.

This chapter presents the development of an AMI infrastructure that integrates seamlessly with the microgrid's communication infrastructure, which was presented in Chapter 2. The developed AMI consists of several modules: smart meters, a communication interface, and HAN gateway. The developed smart meter has a high sampling rate for increased accuracy and is modular. That is, it supports measuring single and three-phase electrical quantities. Since microgrids contain their own renewable resources, the developed smart meter firmware has the capability to track individual sold and consumed power. The firmware also has the capability to calculate the root mean square value of voltages and currents, active and reactive power. The smart meter monitors the power quality by separately evaluating the harmonic components' active and reactive power. The smart meter is designed to flexibly integrate with the utility and microgrids through different communication interfaces. It supports power line communication, ZigBee, and Wi-Fi. Power line communication and ZigBee can be utilized to integrate with the utility, whereas Wi-Fi is utilized to integrate with HAN. The HAN receives the data from the smart meter over an encrypted communication channel for securing private customer information. To provide an interoperability layer, the HAN gateway will share this data with the DDS global data space.

3.2 AMI System architecture

The AMI infrastructure is made up of a communication network, hardware and software components. Figure 3.1 shows an overview of the main AMI system components, which consists of meters, communication network, data concentrators, smart meter head-end and metering data management system MDMS. These system

components enable collection, storage, and management of detailed time-based users' consumption information by the utility companies. The two-way communication network allows transmitting information, such as real-time price, from the utility company to the consumers. The details and functionality of each component are discussed in the next sections.

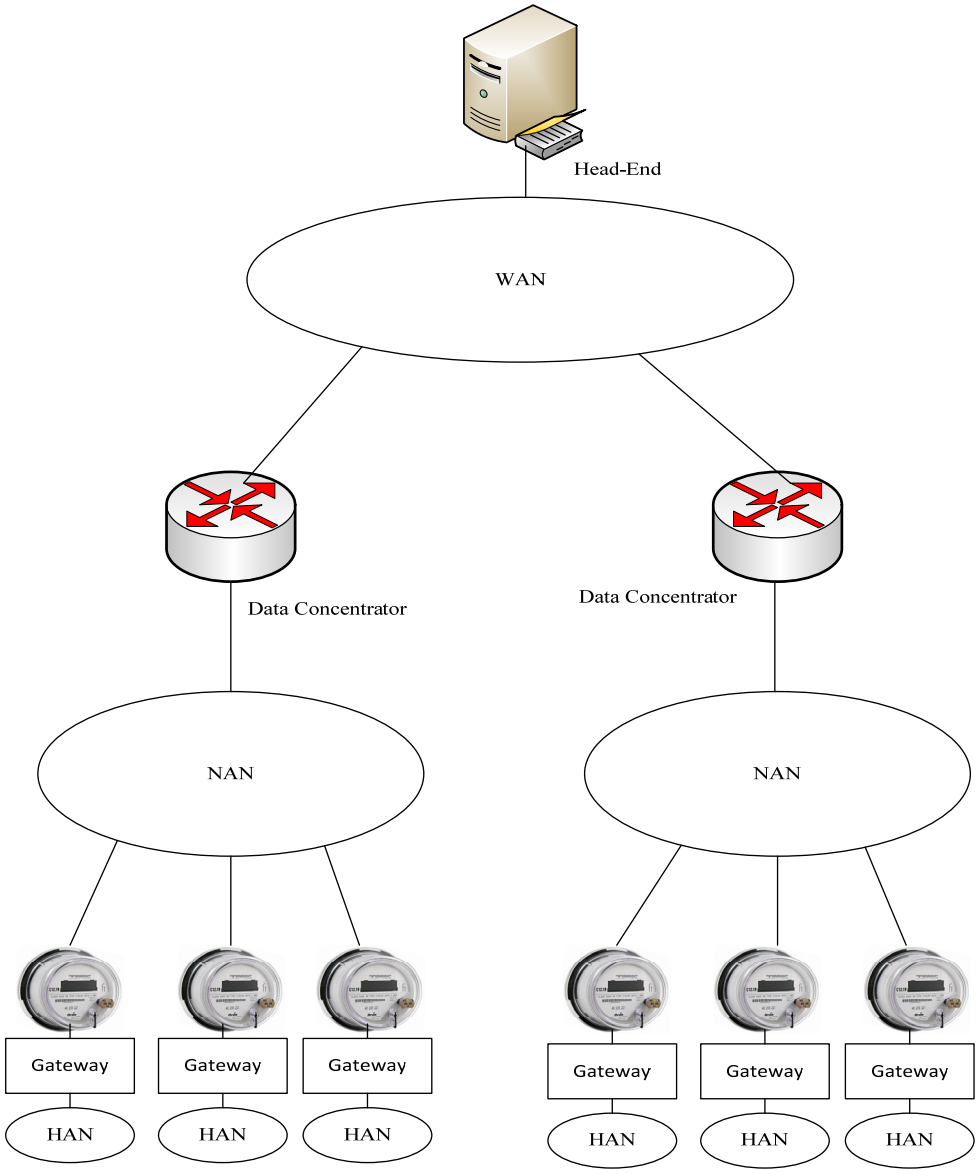


Figure 3.1: Smart meter infrastructure architecture

3.2.1 Smart Meter

The smart meter is a digital device installed in the customers' premises to collect time-based consumption data, such as electricity, water, and gas consumption. The electricity smart meter consists of analog front-end, digital processors, and a communication interface, as shown in Figure 3.2. The analog front-end is comprised of voltage and current transducers, signal condition, filtering circuits, and analog to digital interface. The signal condition and filtering circuits isolate the noise from the measured signal and ensure a proper voltage level before the analog-to-digital conversion stage. The analog to digital convert measured analog signal to a digital stream to be processed by the digital processor.

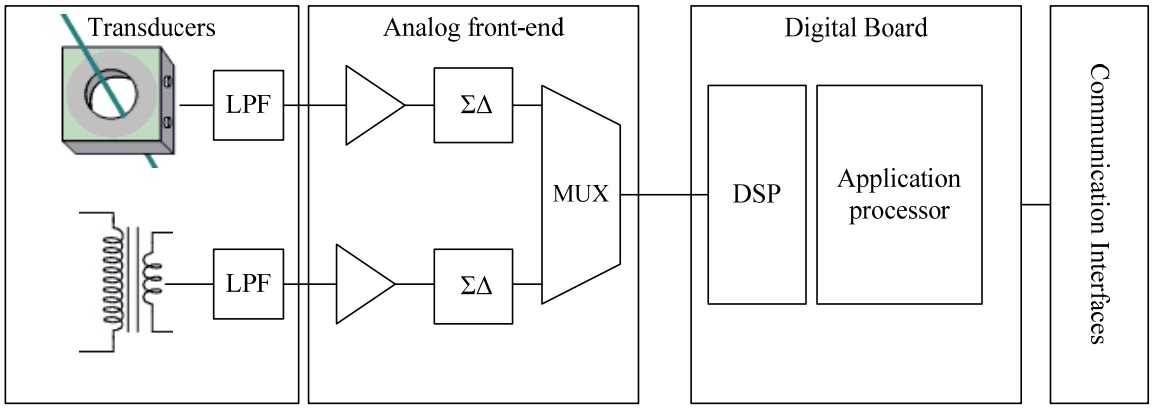


Figure 3.2: Smart meter block diagram

Smart electricity meters usually utilize two different types of digital processors. The first processor is a dedicated digital signal processor, which is designed to perform certain types of calculation. This type of the DSP processor is used to calculate active and reactive energy, harmonic distortion and root mean square voltage and current.

The IEC 62053 standard limits the measurement error for class 1 meter (meters with maximum 40A) to 1% of full scale.

The second processor is a general purpose processor or microcontroller. This type of processor is used to run the smart meter firmware that handles the communication tasks, user interface and store the accumulated energy consumption.

The communication interfaces allow the smart meter to exchange the information with the utility or customer HAN. The most common network interfaces with the utility side are a radio frequency (RF), power line communication, broadband over power line and cellular networks. For the HAN side communication, Wi-Fi and ZigBee wireless network are utilized to connect with the customers' devices and systems.

3.2.2 Communication network

The AMI communication network consists of HAN, Neighbors Area Network (NAN) and WAN. As shown in Figure 3.1. The HAN is a network owned and operated by the end customer. Smart appliances, distributed energy resource controllers, energy and building management systems can exchange information with the smart meter through the HAN gateway. End-customer can grant the utility to control their appliances connected to the HAN network. For example, the utility can throttle pool heater or HVAC systems during peak hours to reduce the load demand. Smart appliances and systems can control the energy demand based on the real-time pricing information. The NAN network aggregates the data from a group of smart meters to the data concentrator. Power line communication or mesh network, such as ZigBee or mesh Wi-Fi, are used to aggregate the data in the NANs.

The WAN network is used to aggregate the data from the data concentrators to the smart meter head-end. The WAN network utilizes power line communication, fiber optics, digital subscriber line or broadband wireless link as backhaul between data concentrators and smart meter head-end.

3.2.3 Data concentrator

The data concentrator is a communication node that collects data from smart meters in the NAN network and aggregates it to the smart meter Head-end. The data concentrator has two network interfaces, one to communicate with smart meters, for example, ZigBee interface, and one to communicate with the WAN network, such as fiber optics or broadband link.

3.2.4 Smart meter Head-end

The smart meter Head-end is a software package that provides a bridge between the AMI and the utility IT network. The Head-end monitors meters' status and collects meters' readings, events and sends remote connection and disconnection command to smart meters. The data collected by the Head-end are stored, managed and analyzed by the MDMS.

3.3 Development of Smart Meter

The developed smart meters are based on the STMPC1 Polyphase energy metering chip from STMicroelectronics. The digital processor and power line communication are based on the STEVAL-IPP001V2 Evaluation Kit shown in Figure 3.3. The STEVAL-IPP001V2 provides the base hardware for the power line modem and 32-bit arm cortex M4 microcontroller. A custom firmware drivers and application were developed to the

process the measured data, manage the communication interfaces, energy calculation and provide the user interface for configuration and calibration. The details of the hardware and software are discussed in the following sections.

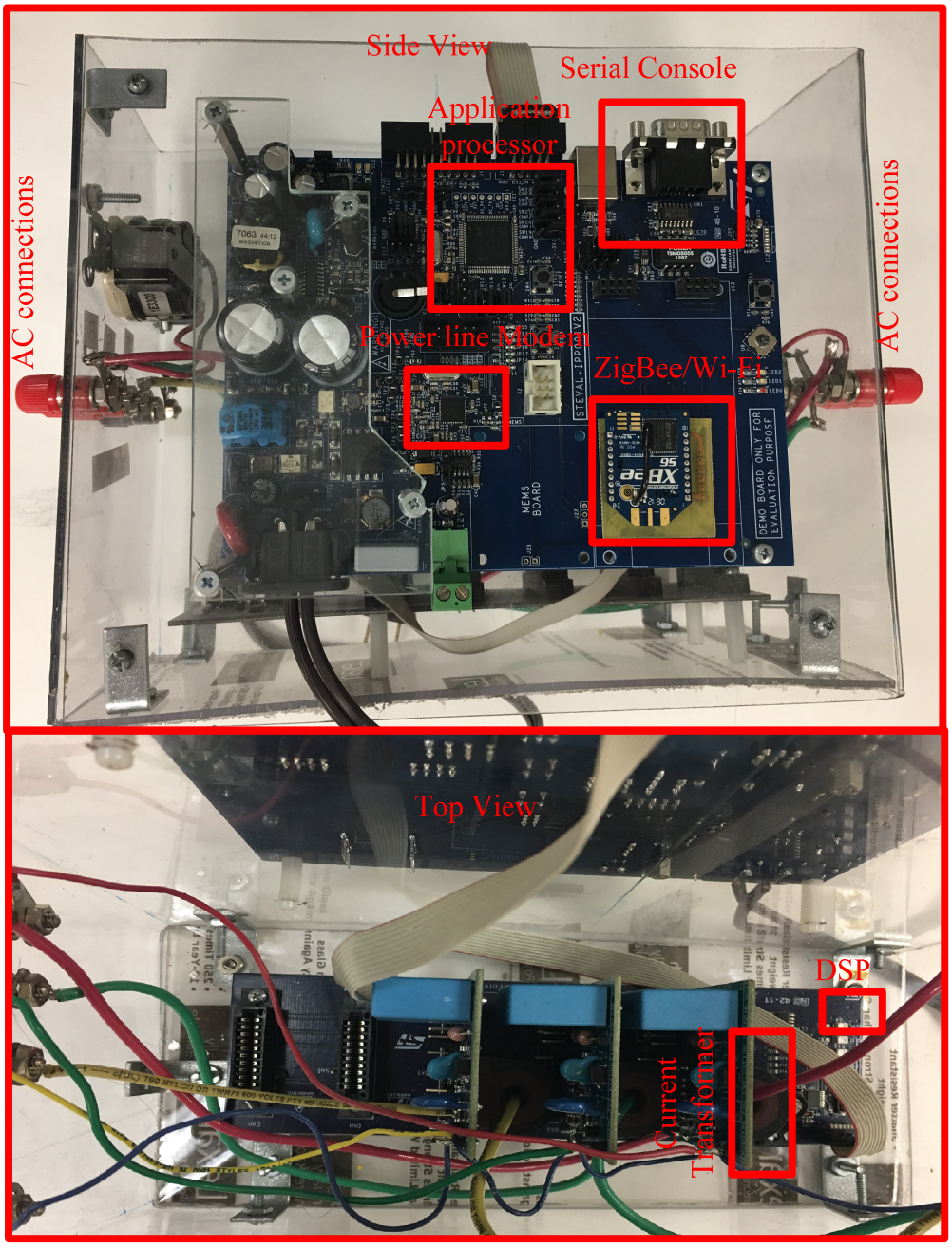


Figure 3.3: smart meter digital processing and communication board

3.3.1 Voltage and current acquisition

The phase voltage and current are measured using a voltage divider and a current transformer, respectively. A current transformer with a maximum current 20A and current ratio 1:2000 is used to measure the phase current. The output current is converted to a voltage using a shunt resistor. An RC filter is used to filter the noise and limit the signal bandwidth before the analog conversion stage, as shown in Figure 3.4. The analog front end and digital conversion are based on the STMPS2 second order sigma delta modulator with programmable gain amplifier and built-in accurate voltage reference. The STMPS2 samples the voltage and current input channels simultaneously with 2 MHz sampling rate per Chanel. Two sigma delta modulators convert the sampled analog measurement to a stream of bits. The voltage and current bit streams are multiplexed to a single 4 MHz bit output channel. The STMPS has a 0.5% error over the full scale, which is below the standard limit. The IEC 62053 class 1 (meters with 40A max current) allows 1% error.

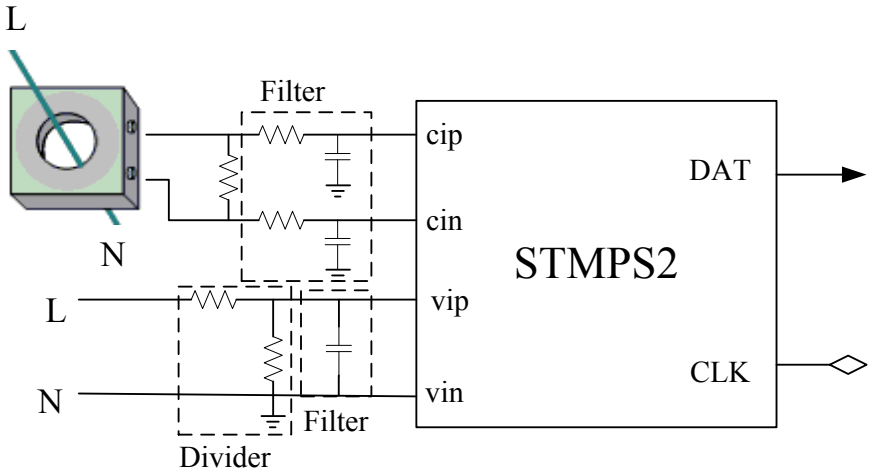


Figure 3.4: current and voltage transducers connection diagram

For a polyphase meter, an STMPS2 chip is used for each phase.

3.3.2 Signal processing and power calculation

A dedicated digital signal processor (STMPC1) is used for energy calculations. The STMPC has four DSP engines that process the measurements from the three phases in addition to neutral current. The DSP engines check the integrity of the digital streams produced by the analog front-end and compute the cumulative active and reactive energies, cumulative active and reactive fundamental energies, RMS values for voltage and current, and line frequency. The STMPC1 implements a tamper detection algorithm to detect energy theft. The tamper detection module monitors the sum of the current, phase sequence, active power direction, and electromagnetic interference. All computed energies, voltage and current measurements, and internal registers can be accessed by the application processor through SPI bus. Figure 3.5 shows the connection diagram for the STMPC1, analog front-end, and the application processor.

To calibrate for the error due to component tolerance and measurement error, the DSP engines have calibration registers that can adjust the readings by ±12.5%. Calibration values can be stored temporarily in shadow registers or permanently in one-time programming (OTP) memory. The DSP engine can read the calibration value from the OTP or temporary memory by setting the RD signal. If the RD signal is set, the configuration bits will be loaded from shadow registers otherwise, if RD is cleared, the configuration bits will be loaded from the OTP memory. This allows testing the configuration before permanent writing to the devices' OTP memory. However, this allows the software to load different calibration values to the shadow registers and switch

the configuration from OTP to shadow registers. During our test, we were able to connect a small circuit between the application processor and the STMPC1. This circuit simply loads the wrong calibration value to the shadow registers and switches the RD signal to load the configuration from the shadow registers. The circuit transparently passes the reading commands and data between the application processor and the STMPC1. By modifying the shadow registers, the power consumption can be reduced by 12.5%. To avoid this type of vulnerability, the DSP engines should allow disabling the shadow register permanently after writing configuration bits to the OTP memory. Moreover, an authentication mechanism is required between the application processor and the DSP engines.

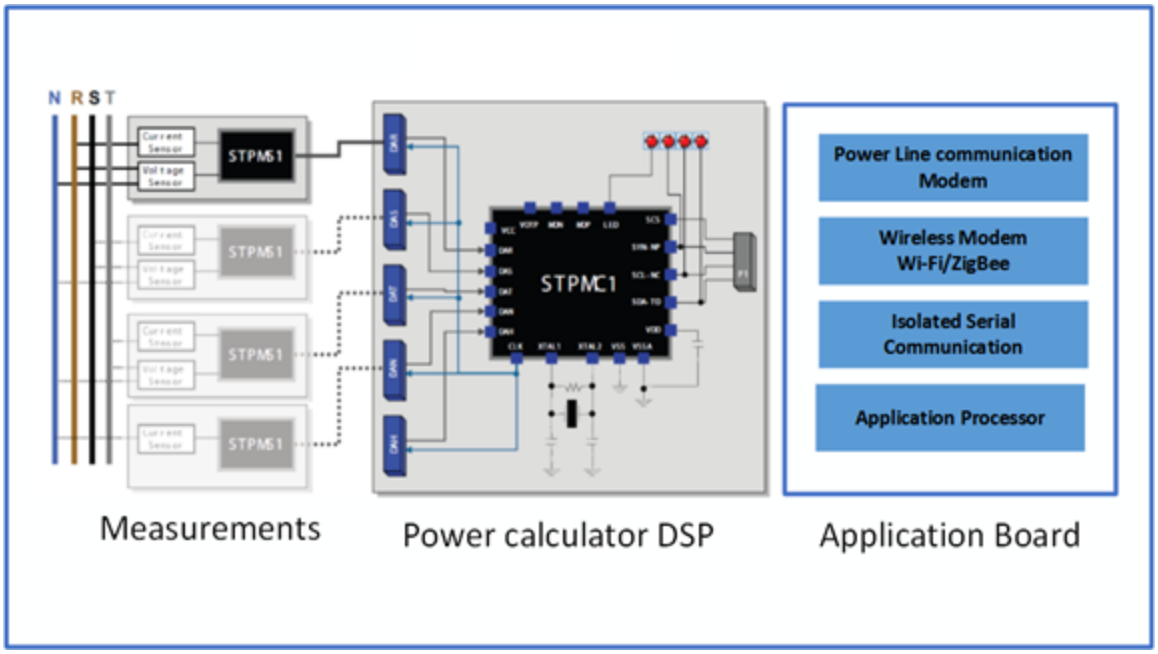


Figure 3.5: Energy computing DSP engine connection diagram

3.3.3 Communication Modules

Three types of communication modules are used in the developed smart meters. The first module is a power line communication interface. The power line communication is based on the ST7580 narrow-band power line networking chip designed to work in CENELEC A and B band. The ST580 provides a data rate up to 28.8 Kbps with PSK modulation. The application processor communicates with the power line networking chip using the universal asynchronous receiver/transmitter (UART) port. The data link layer implemented in the ST580 provides error detection of corrupted frames in addition to encryption and authentication based on the 128 bit AES encryption algorithm. The block diagram for the ST580 and connection with the application processor is shown in Figure 3.6.

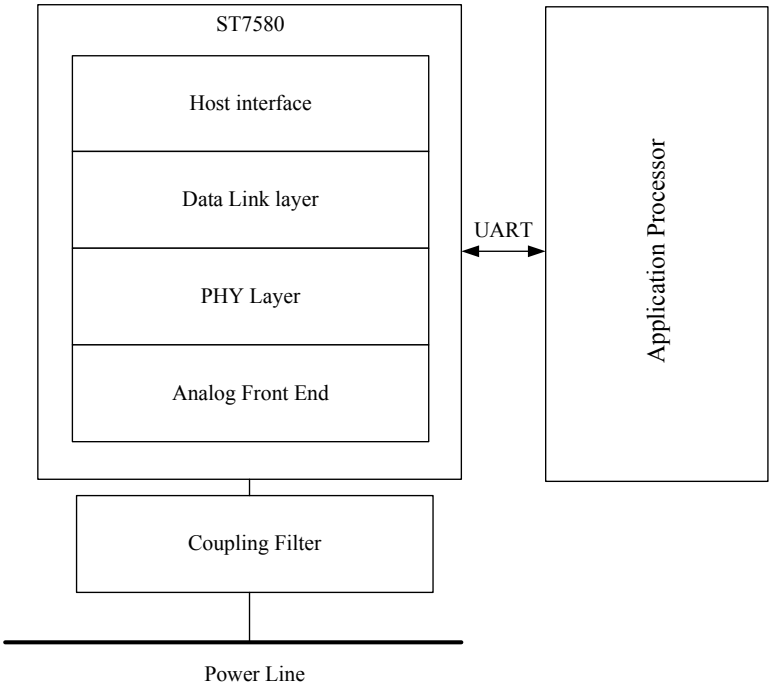


Figure 3.6: Power line modem block diagram

The second communication module is the XBee S2C ZigBee module. The S2C module supports peer-to-peer or wireless mesh network configuration. Mesh network allows the smart meters to relay the messages from remote meters to the data concentrator. The ZigBee module can be used as an alternative to power line network to communicate with the utility or the customer gateway. Communication over ZigBee wireless network is encrypted using AES 128 bit encryption.

The third communication module is a Wi-Fi module. The Wi-Fi module is interchangeable with the ZigBee module. If both Wi-Fi and ZigBee modules are required, the Wi-Fi module can be connected to the isolated RS-232 port using an RS-232/TTL adapter.

3.3.4 Smart meter firmware

Custom firmware is developed to operate the smart meter. The firmware code is developed using C language and compiled using a C cross compiler for ARM cortex M4. The firmware is divided into three different layers, as shown in Figure 3.7. The low-level layer implements the hardware driver and low-level functions, such as basic input/output and hardware peripheral initialization. The low-level drivers include the STMPC1 driver, communication modules drivers, and serial console driver. The middle layer implements data extraction functions, communication protocols and data structures, calibration and configuration functions. The top layer represents the application layer, which performs energy accumulation, energy price exchange, controls smart appliances and remote disconnection.

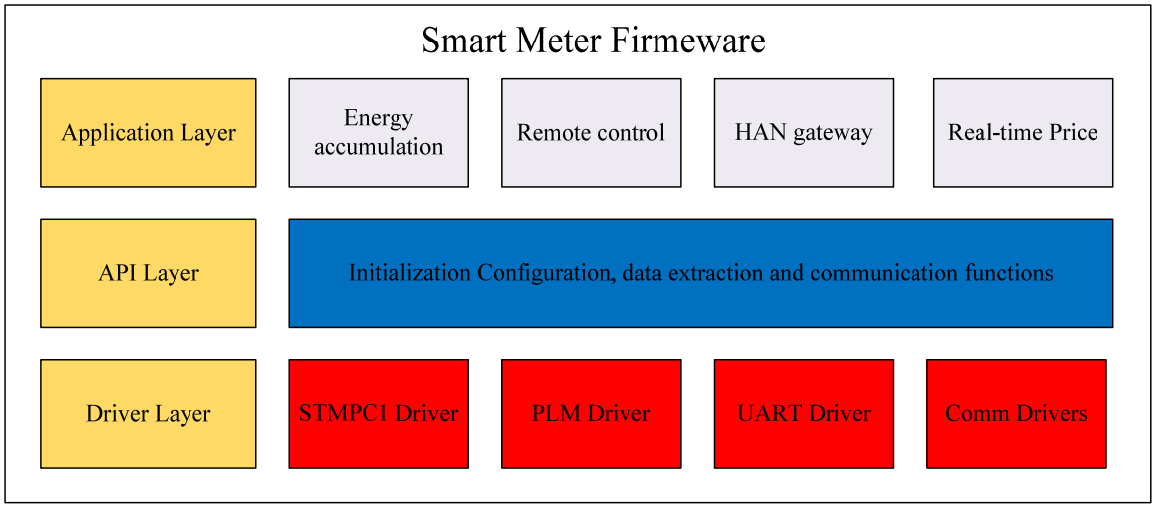


Figure 3.7: Smart meter firmware architecture

3.3.4.1 Developed firmware functions

DSP engine and communication modules are connected to the application processor through either Serial Peripheral Interface (SPI) bus or UART. Low-level drivers provide the basic function to initialize, read or write data to the SPI and UART modules. The initialization functions allow setting the data rate and data length (number of bits). Basic input/output functions allow sending, receiving and validating single data word.

The STMPC1 driver calls low-level SPI input/output functions to access the STMP1 internal registers. The STMPC_Init() function initializes the connection with the STMPC1 chip, configures voltage and current transducers types and loads the calibration data to the shadow registers.

The STMPC1's data registers are organized in seven different groups[58]. Each group consists of four 32 bits data records, as shown in Figure 3.8. Each record contains 4 bits data parity and 28 bits data fields. The data records are described as below:

- **Group 0 data records:** this group consists of four data records DAP, DRP, DFP, and PRD. The DAP and DRP records contain the three-phase active and reactive energy produced by harmonic and fundamental components. In addition to the energy records, DAP and DRP contain 12 status bits. The DFP record contains the three-phase energy produced by the fundamental component. The PRD record contains the time period measured for one cycle and DC component.
- **Group 1 data records:** this group consists of DMR, DMS, DMT and DMN data records. The DMR, DMS, and DMT contain the instantaneous measurement of the three-phase voltages and currents. The DMN data record contains the sum of the three phase voltages and current.
- **Group 2 data records:** this group consists of DER, DES, DET and DEN data records. The DER, DES, and DET contain calculated RMS values of the three-phase voltage and currents, while DEN contains the RMS value of the neutral current.
- **Group 3 data records:** this group consists of DAR, DAS, DAT and CF0 records. The DAR, DAS and DAT records contain the active energy for phases R, S, and T, respectively. The CF0 record contains configuration bits.
- **Group 4 data records:** this group is similar to Group3 except that DRR, DRS and DRT records contain the reactive energy of phases R, S and T, respectively. The CF1 record contains configuration bits.
- **Group 5 data records:** this group consists of DFR, DFS, DFT and CF 2 records. The DFR, DFS and DFT records contain the fundamental active

energy for phases R, S, and T, respectively. The CF2 record contains configuration bits.

- **Group 6 data records:** this group consists of ACR, ACS, ACT and CF3 data records. The ACR, ACS and ACT records contain the accumulated Ah for phases R, S and T, respectively. The CF3 record contains configuration bits.

To simplify reading and interpreting the data records, the developed driver provides a simple function to read the data records. The Read_Register() function reads the contents of the seven data records and stores the content in a data structure. The data records contain digital counts that represent measured voltages, currents, and energies. These digital counts can be interpreted to voltage, current and energy values based on the system design parameters, such as the current transformer ratio, programmable amplifier gain, and configuration bits. The developed driver provides a set of functions to extract and interpret the records digital counts to real values for voltage, current, and energy. The data extraction functions are described as below:

- "PQ_3phase_Extraction()": this function processes the data record and returns the sum of the three phase energy, reactive energy, and fundamental energy accumulated in the data records. The data records must be read frequently to avoid data loss due to registers overrun.
- "IRMS_Extraction()": this function returns the RMS values for the three-phase currents.
- "VRMS_Extraction()": this function returns the RMS values for the three-phase voltages.

- “P_RST_Extraction()”: this function returns the individual accumulated energy for phase R, S, and T, respectively.
- “Q_RST_Extraction()”: this function returns the individual accumulated reactive energy for phase R, S, and T, respectively.
- “Total_energy()”: this function returns the total consumed, supplied and net energy. The developed smart meter can accumulate the load change with a minimum load equal to 7.2mw/h.
- “Total_reactive_energy()”: this function returns the total reactive energy.
- “Total_fundmental_energy()”: this function returns the total consumed, supplied and net fundamental energy.
- “R_energy()”: this function returns the consumed, supplied and net energy for phase R.
- “S_energy()”: this function returns the consumed, supplied and net energy for phase S.
- “T_energy()”: this function returns the consumed, supplied and net energy for phase T.

  Higher level functions are developed to format the data frames, transmit the data over communication links and respond to Head-end requests. A serial console is developed to print debugging and status messages. The operator can use the serial console interface to change the meter and communication parameters, such as encryption keys, communication speed, and calibration data.

	Group 0 Data records			
DAP	Parity (4 bit)	3-phase active energy (20 bit)	3-ph lower status	
DRP	Parity (4 bit)	3-phase reactive energy (20 bit)	3-ph up status	TSG bits
DFP	Parity (4 bit)	3-phase active energy (fundamental) (20 bit)	System signals	
PRD	Parity (4 bit)	Period (12 bit)	DC (12 bit)	
	Group 1 Data records			
DMR	Parity (4 bit)	Phase R Voltage (12 bit)	Phase R current (16 bit)	
DMS	Parity (4 bit)	Phase S Voltage (12 bit)	Phase S current (16 bit)	
DMT	Parity (4 bit)	Phase T Voltage (12 bit)	Phase T current (16 bit)	
DMN	Parity (4 bit)	Some of all currents	Neutral current (16 bit)	
	Group 2 Data records			
DER	Parity (4 bit)	Phase R Voltage RMS (12 bit)	Phase R current RMS (16 bit)	
DES	Parity (4 bit)	Phase S Voltage RMS (12 bit)	Phase S current RMS (16 bit)	
	Group 3 Data records			
DAR	Parity (4 bit)	Phase R Active energy (20 bit)	R-phase status	
DAS	Parity (4 bit)	Phase S Active energy (20 bit)	S-phase status	
DAT	Parity (4 bit)	Phase T Active energy (20 bit)	T-phase status	
CF0	Parity (4 bit)	Bits[27-0] of configurations		
	Group 4 Data records			
DRR	Parity (4 bit)	Phase R Reactive energy (20 bit)	R-phase status	
DRS	Parity (4 bit)	Phase S Reactive energy (20 bit)	S-phase status	
DRT	Parity (4 bit)	Phase T Reactive energy (20 bit)	T-phase status	
CF1	Parity (4 bit)	Bits[55-28] of configurations		
	Group 5 Data records			
DFR	Parity (4 bit)	Phase R Active energy fundamental (20 bit)	R-phase status	
DFS	Parity (4 bit)	Phase S Active energy fundamental (20 bit)	S-phase status	
DFT	Parity (4 bit)	Phase T Active energy fundamental (20 bit)	T-phase status	
CF2	Parity (4 bit)	Bits[83-56] of configurations		
	Group 6 Data records			
ACR	Parity (4 bit)	Phase R Current Ah (20 bit)	R phase delay	
ACS	Parity (4 bit)	Phase S Current Ah (20 bit)	S phase delay	
ACT	Parity (4 bit)	Phase T Current Ah (20 bit)	T phase delay	
CF3	Parity (4 bit)	Bits[111-84] of configurations		

Figure 3.8: STMPC1 data record

3.3.5 Development of data concentrator and smart meter Head-end

To collect and manage the data from multiple smart meters, smart meter Head-end software is developed based on the NI LabView graphical programming environment (see Figure 3.9). Each smart meter sends a data frame that contains energy, voltage, and current data. The message frame contains a unique identification code for each meter. The head-end software publishes collected data to a DDS domain dedicated to smart meter data. The published data object contains all consumption and measured data, in addition to the meter ID. The smart meter GDS domain is monitored by a database service that stores all published data object to a database. The head-end software can send a price signal and control command to the smart meter.

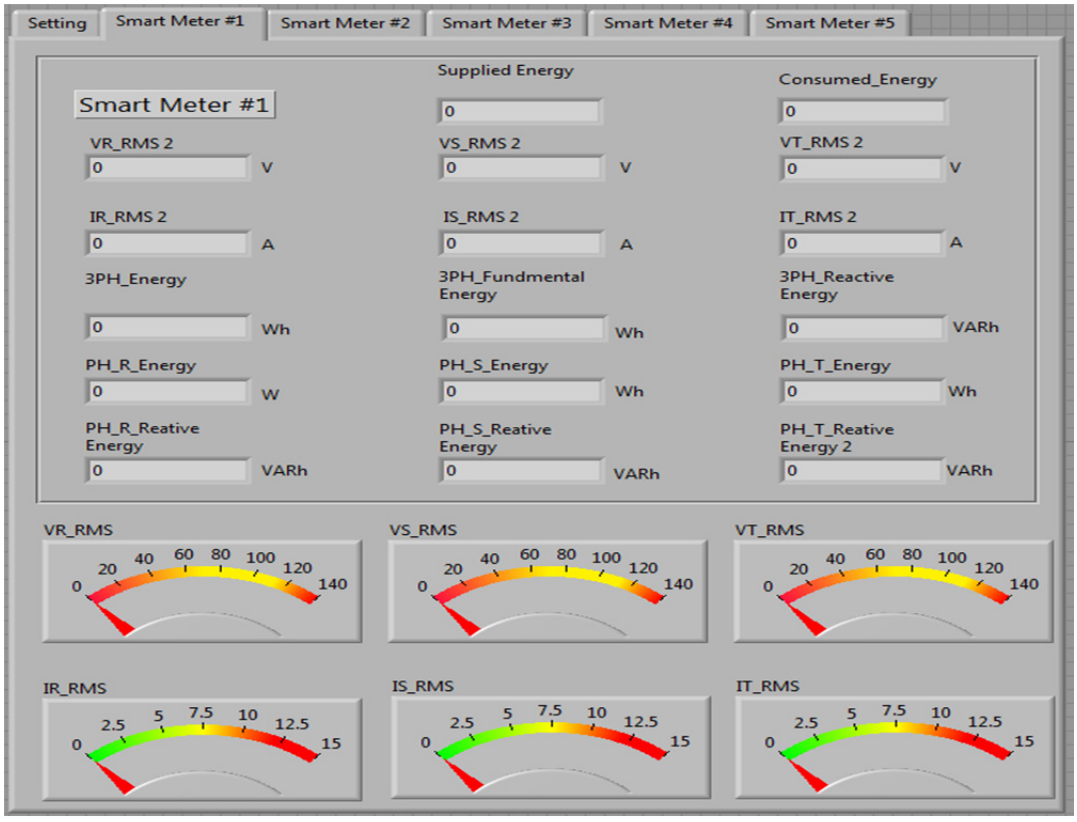


Figure 3.9: smart meter head-end interface

3.3.6 Development of HAN Gateway

To exchange information with the HAN, a gateway is developed using the BeagleBone single board Computer (SBC). The SBC runs an embedded Linux operation system and the HAN gateway software. The gateway software is developed using C programming language. The software periodically polls the consumption and price information from the smart meter using a WiFi communication link and publishes this information to the microgrid domain. The published information is accessible by the microgrid applications and devices, such as the energy management system. Separate smart meters domains and data flow are shown in Figure 3.10.

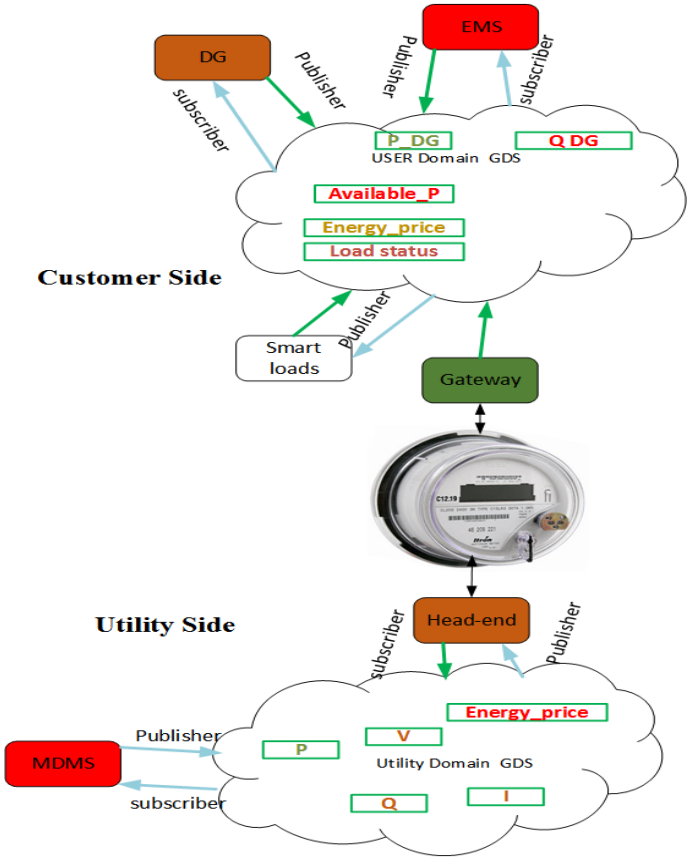


Figure 3.10: Data flow between customer and utility domains

3.4 Summary

In this chapter, an AMI infrastructure is developed and integrated with the smart grid testbed. The developed AMI has a flexible communication interfaces that allow connections with ZigBee, WiFi, and powerline communication networks. Unlike the commercially available meters with proprietary software, development of custom firmware and application allows modification, implementations and testing new algorithms and ideas. The developed AMI is seamlessly integrated with the developed communication infrastructure.

Chapter 4 Synchronized measurement network

4.1 Introduction

Electric power systems are undergoing profound and radical changes triggered by the advent of new technologies not only in generation and storage, but also in power electronics, sensing, control, computing, and communications. Specifically, they are evolving toward more flexible Microgrids infrastructures. Modern grids encounter high penetration of renewable energy and distributed resources. Most of these will be installed on the distribution networks. Current distributions networks are designed as radial networks for unidirectional power flow. With passive customers (i.e. customer only consumes power), the designer only considers the maximum limits, such as maximum loads and short circuit current, rather than real-time sensing the operating conditions [59]. With the high penetration of renewable energies, energy storage, and plug-in electric vehicles, it's necessary to continuously monitor the magnitude and phase angle of the voltages and current to control the power flow, damp power oscillation and maintain distributed sources synchronization. Direct measurements of the voltage and phase angle can be achieved by utilizing phasor measurement units and GPS time reference. Phasor measurement units are usually deployed in transmission networks. The phase difference in the distribution network is much smaller compared to the phase difference in transmission systems. Phase measurement in the distribution network requires higher resolution measurements units. Micro-Synchrophasor is developed with a higher resolution for distribution network installation [60]. In this chapter, a development of low-cost high-angle resolution synchronized measurement unit will be introduced. The

proposed measurement unit utilizes the DDS communication middleware to support completely distributed and resilient peer/peer communication environment. The measurement unit can directly measure the phase angle, frequency and the magnitude of the voltage and current fundamental components.

4.2 Synchrophasor measurements

Synchrophasor units provide time-stamped measurements with high accuracy time reference in order to compare different measurements from different sites or locations. Time-stamped measurements make it possible to directly measure the phase angles between bus bars or feeders voltages. The block diagram of the synchrophasor measurement unit is depicted in Figure 4.1. First, the analog measurements are filtered using low pass filter before the analog to digital conversion. An antialiasing filter with a bandwidth equal to half of the sampling frequency is used to limit the signal bandwidth and prevent aliasing. A global positioning system (GPS) receiver provides a common time reference for the system. The GPS time reference has low frequency, typically 1 Hz. A higher rate clock is produced from the GPS 1 Hz reference using Phase Locked Loop (PLL). This clock drives the ADC sampling rate and synchronizes the microprocessor instruction execution. In addition to the 1Hz time reference, the GPS provides the current universal time (UTC) using serial or IRIG protocols. The digital processor time stamps the collected samples with the GPS time and calculates the phase angle relative to the cosine function at the nominal system frequency synchronized to the UTC clock. Time-stamped data are transmitted using the network interface to the phasor data concentrator PDC. The PDC collects the data from multiple phasor measurements units, correlates the

data by the time tag and retransmit it to the higher level application or supper PDC, which collect the data from multiple PDC. Phasor data are exchanged using IEEE C37.118.2 or IEC 61850-90-5. The IEC 61850-90-5 standard uses a UDP multicast to deliver the phasor data to the subscriber.

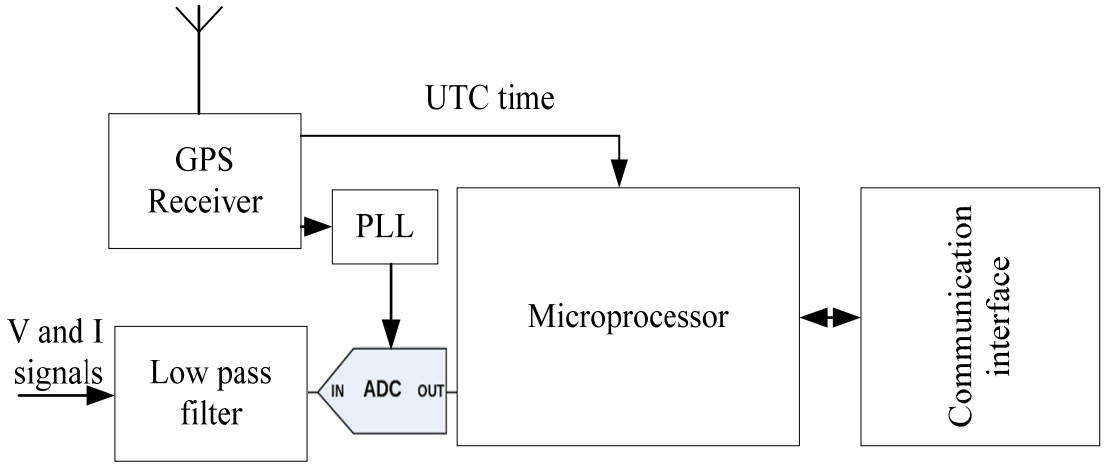


Figure 4.1: Phasor measurement unit general block diagram

The developed measurement unit consists of three different Modules, analog module, digital module, and a communication module. The construction and operation details of the three modules are described in the next sections.

4.3 Analog interface module

The analog interface module consists of six analog filters and six analog comparators. The analog filters are an identical low-pass filter that limits the bandwidth of the measured voltage and current signals, see Figure 4.2. Since we are interested in the fundamental component phase angle only, the low pass filter is designed to pass the frequency from 10 to 140 Hz. This bandwidth is suitable for both 50Hz and 60Hz system. The frequency response of the low-pass filters is shown in Figure 4.3. As depicted from the figure, the filter has a unity gain in the passband region. The filter attenuates the third

and fifth harmonics order with 40db and 70db, respectively. The filtered signals are connected to six analog comparators (see Figure 4.4: Analog comparators). The analog comparator converts the sinusoidal waveform to a square waveform. The leading edge of the square wave is synced with the positive zero crossing of the sinusoidal signal. To minimize the phase error between the sinusoidal signal and generated square wave, an ultrafast 4.5 Nanosecond analog comparator is used. High slew rate makes it possible to generate a sharp edge square wave with neglected phase delay relative to the sinusoidal signal. The slew rate for the analog comparator will produce maximum phase error equal to 9.72e-05 degree.

4.4 Digital processing modules

The digital processing board consists of ARM cortex M4 32 bit microcontroller, phase measurement circuits, GPS receiver and Phase locked loop. The block diagram for the digital processing board is shown in

Figure 4.5. The phase locked loop is adjusted to generate 60Hz output frequency for the 60Hz supply system and 50Hz output for 50 Hz supply system. The phase locked loop output is synchronized with the GPS 1 Hz time reference output. The phase angles between the comparators' square wave outputs and the phase locked loop output represent the relative phase angles between measured signals and GPS clock. To measure these phase angles, a XOR gate is used. The XOR gate inputs are connected to the phase locked loop clock output and the square wave from the comparator. The output pulse duration shown in Figure 4.6 represents the phase angle. As depicted from the figure,

when GPS and the input signal has the same phase shift, the duty cycle of the output is 0%, while the output duty cycle is 100% in case of 180-degree phase shift.

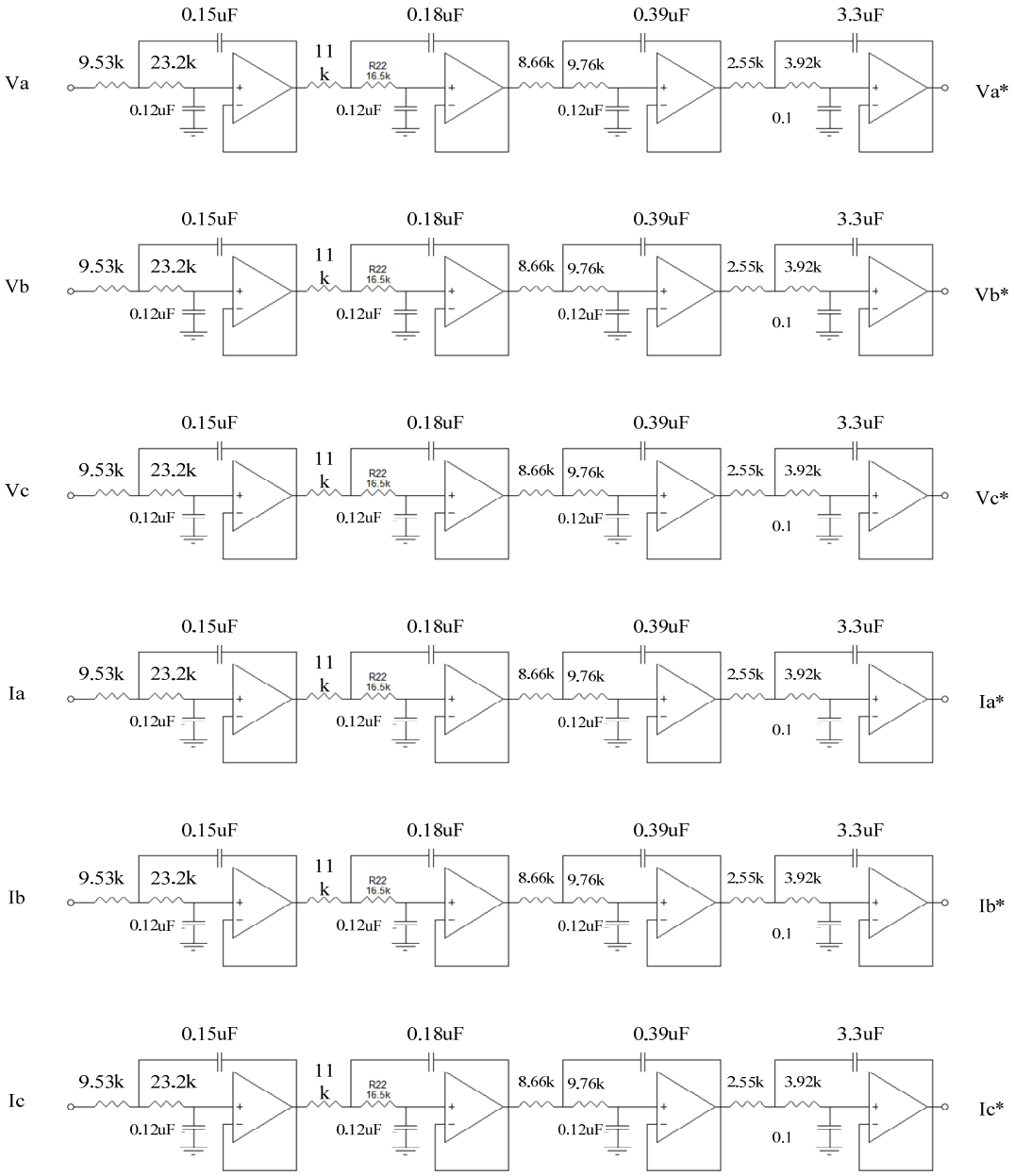


Figure 4.2: analog filter schematic diagram

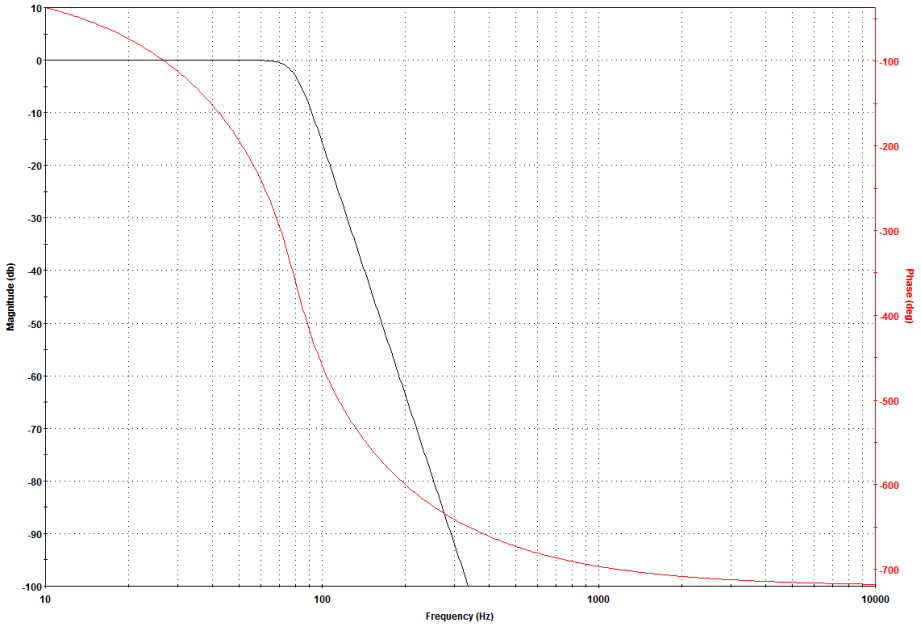


Figure 4.3: analog filter frequency response.

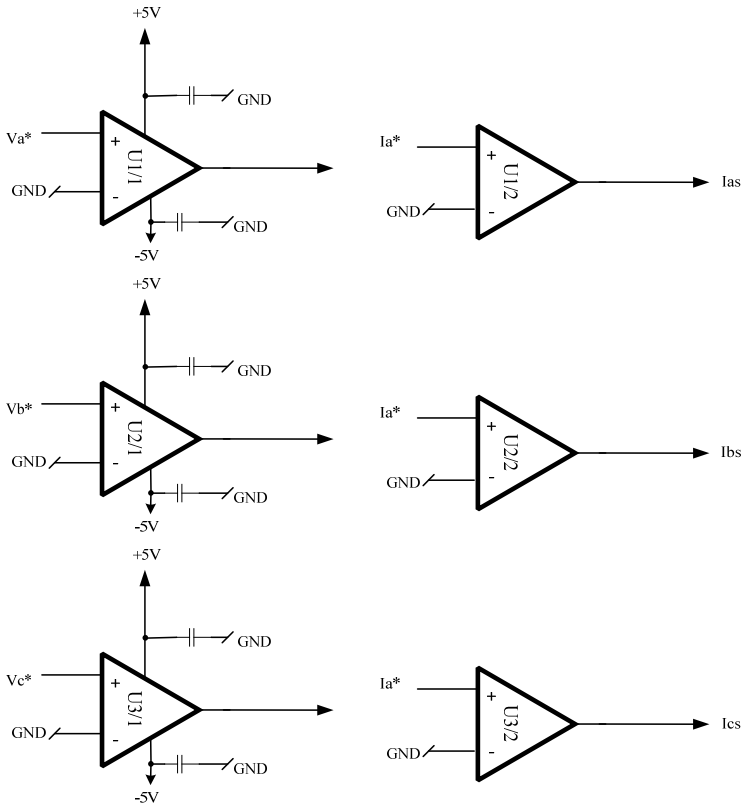


Figure 4.4: Analog comparators

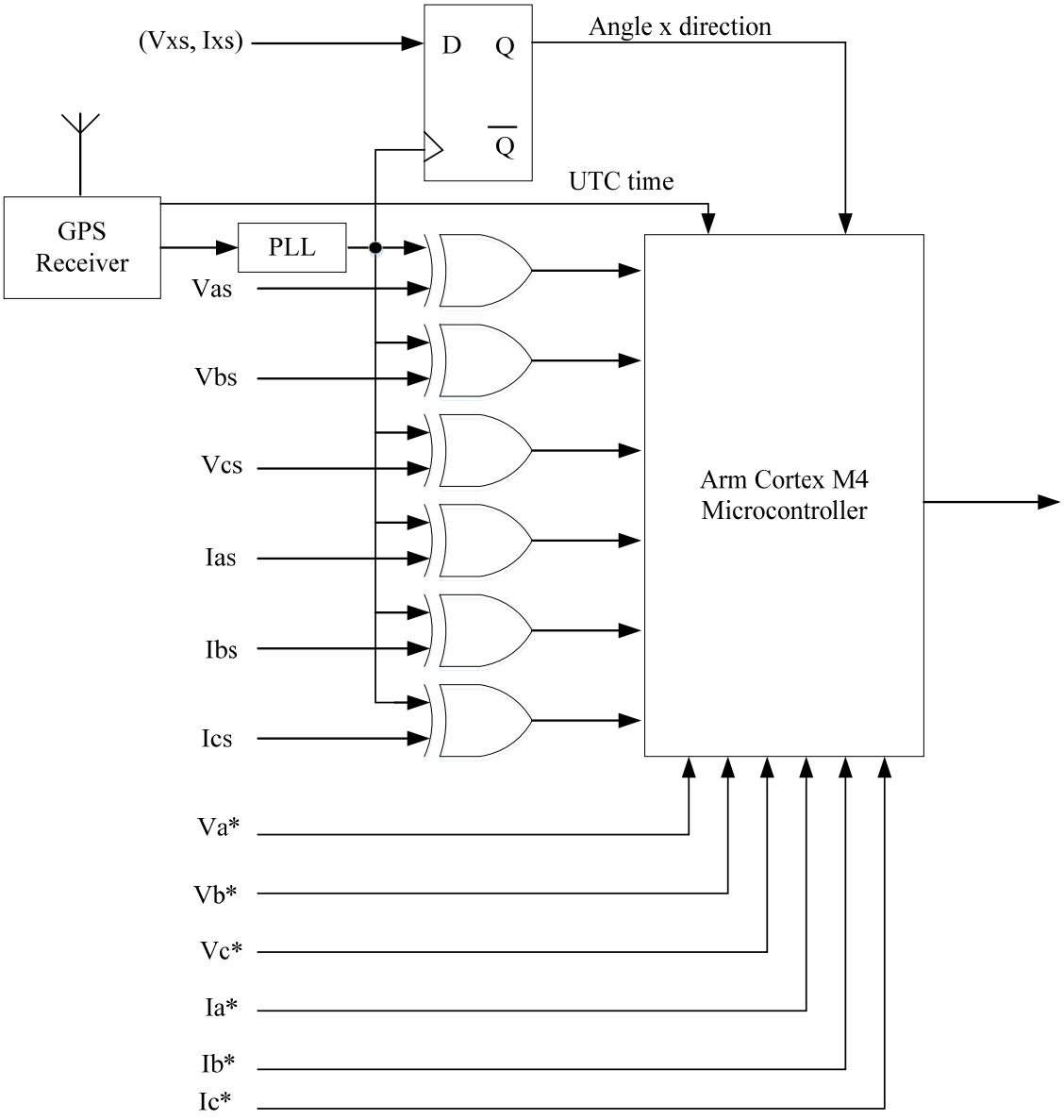


Figure 4.5: Digital processing board block diagram

The XOR output pulse duration accurately represents the phase angle magnitude; however, it doesn't contain information regarding the angle direction. For example, positive and negative 90-degree phase angle will produce the same pulse width output. To detect the angle direction, another circuit is implemented. The direction detection circuit consists of edge triggered D-type flip. The GPS clock reference is connected to the

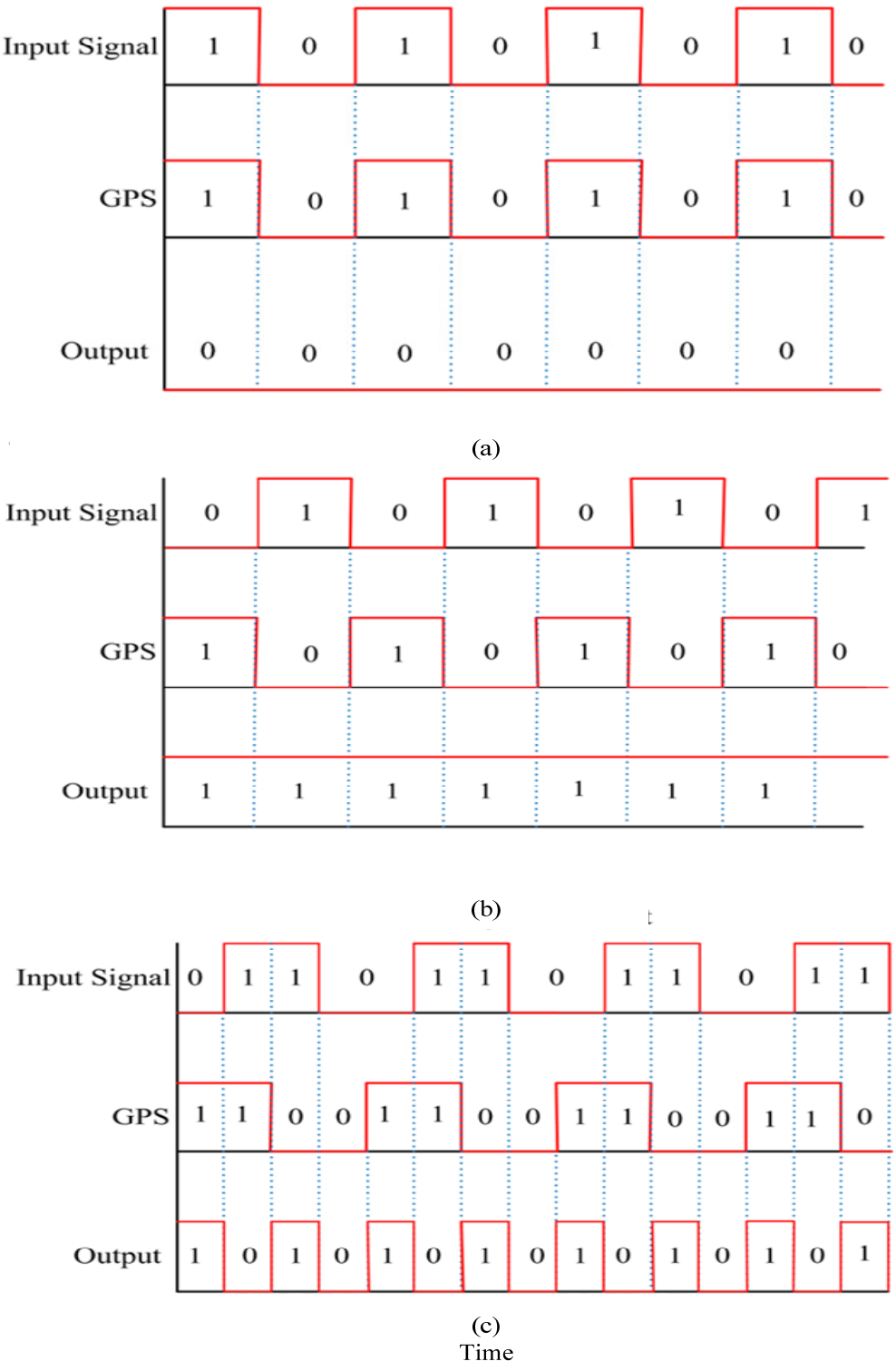


Figure 4.6: Phase comparison with the GPS reference (a) zero degree phase shift, (b) 180 phase shift, (c) 90-degree phase shift

flip-flop clock input while the signal square wave is connected to the D input. If the square signal lags the GPS reference, the GPS clock will always latch zero output while the output will be high if the square signal leads the GPS reference. Figure 4.7 shows the timing diagram for the lead/lag phase detection circuit. The filtered analog signals, phase angle magnitude signals, and phase direction signals are connected to the ARM cortex microcontroller running at the 168MHz clock. The microcontroller converts the voltage and current to a digital form using the built-in analog to digital converter with 12-bit resolution and 10k sample/s. After converting the measured signal to digital form, the microcontroller calculates the voltage and current root mean square values. To read the phase magnitude, a pulse width captured module is used to measure the pulse width and convert it to a digital count. The built-in capture module consists of a 16 bit counter and programmable clock source. The programmable counter can be configured to count the number of the pulse between rising edge, trailing edge and both. To measure the pulse width that represents the phase angle, the modules are configured to count the pulses from the programmable clock sources between rising and trailing edge instances. The clock source is programmed to divide the processor 168MHz clock by 32 to produce 5.25 MHz clock.

With 16 bit counter resolution and 5.25 MHz clock, the pulse capture module can measures an angle from zero to 269.63 degree with 0.0041degree resolution. The microcontroller firmware adds a fixed phase angle to compensate for the phase angle results from the low-pass filter. In addition to pulse width measurement, the pulse

capture module can measure the frequency of the input signal. One capture module is configured to measure the frequency of phase A voltage signal to represent the system frequency. After calculating the phase angle, root mean square voltages and currents, and system frequency, the microcontroller firmware transmit calculated data with the time stamp to the communication module over the high-speed serial interface.

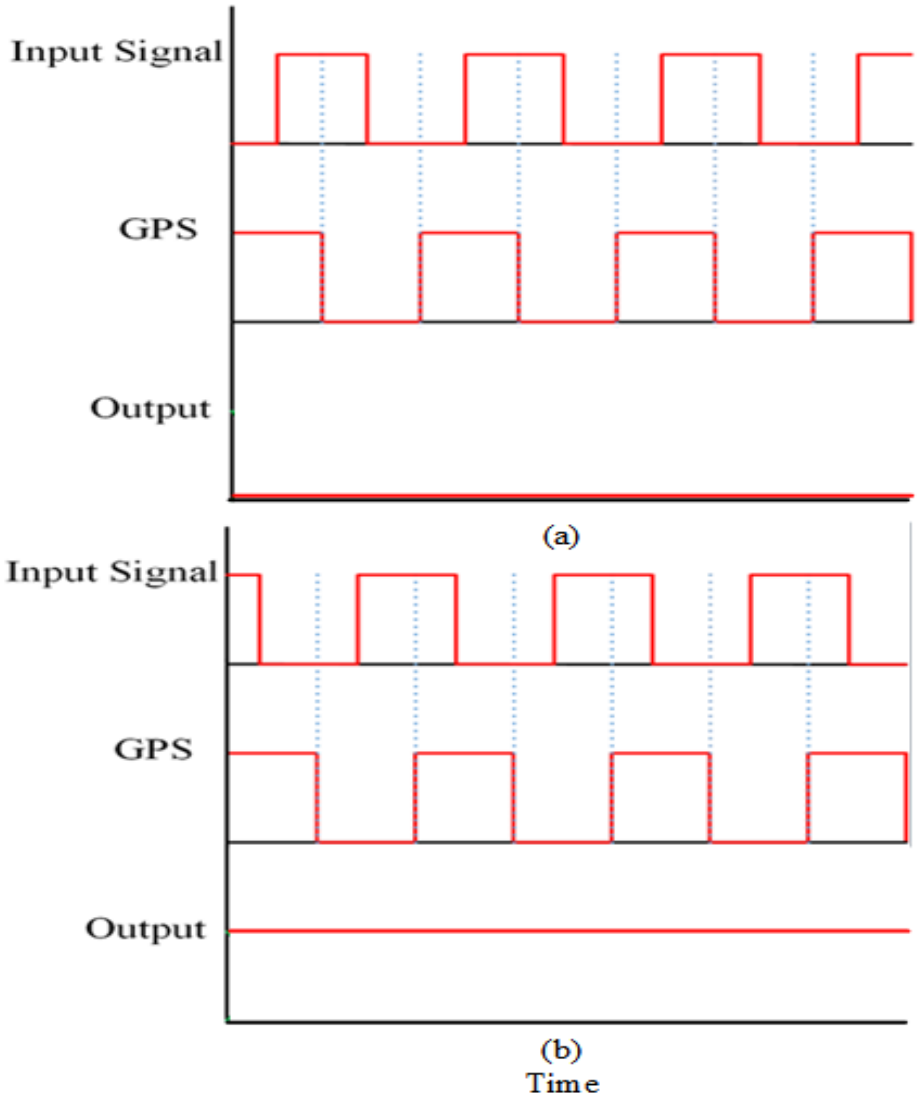


Figure 4.7: Phase detection timing diagram, (a) lag signal, (b) lead signal

4.5 Communication Module

The communication module is based on a SBC with Ethernet, and USB interface. The SBC runs embedded Linux with real-time extension. The embedded Linux provides the necessary hardware drivers for the Ethernet, Wi-Fi and serial interface in addition to the networking TCP/IP stack. The SBC runs a custom-developed software application that collects the measurement from the digital processing board and publishes it to the network using a publisher/subscriber communication scheme.

The developed software utilizes the DDS library from RTI to implement the publisher/ subscriber communication. To minimize the bandwidth required to exchange the information, the software uses UDP multicast messages to deliver the synchronized measurement like the IEC 61850-90-5. The DDS library supports two different quality of service for the message delivery over the UDP packets, best efforts, and reliable communication. In the reliable communication, the RTPS protocol ensures the delivery of the UDP packets to all subscribers. In addition to the UDP multicast, TCP communication is also supported. TCP communication is necessary when passing the data packets over a network that blocks UDP packets, such as communication over internet and cloud communication. In addition, the software supports push oriented and pull-oriented operating modes.

The published data objects are stamped with a current time stamp at the publisher side. Another time stamp is added at the subscriber side when the data is received. The middleware can be configured to arrange received data objects based on the transmission or received time stamp. To eliminate the need for data concentrator to arrange the data

object in the correct timing order, the middleware is configured to arrange the data packets based on the transmission time stamp. The test setup and transmitted data are shown in Figure 4.8. In the test setup, the digital processing board was able to measure the frequency with 0.004Hz accuracy and the phase angle with error 0.01 degree.

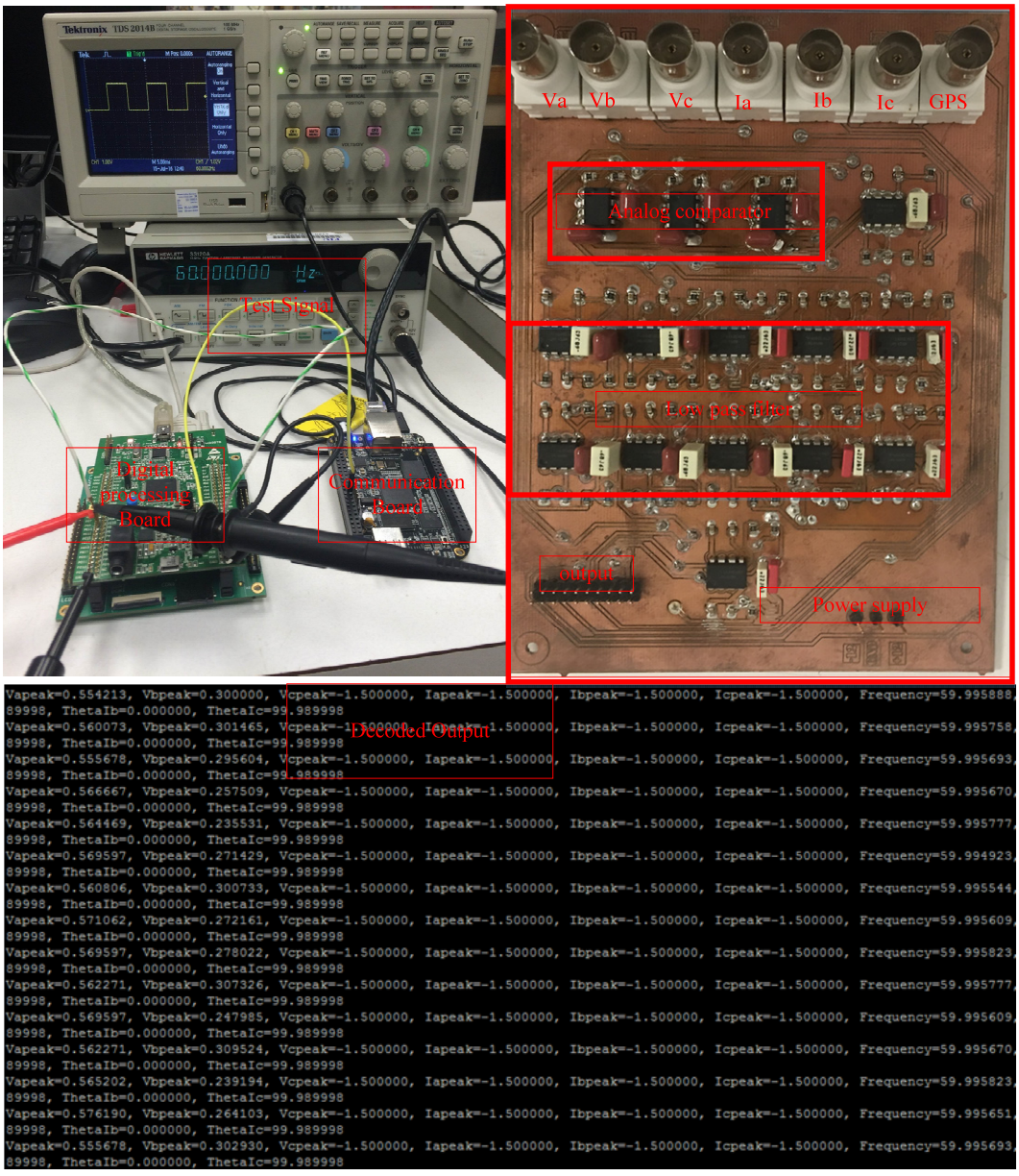


Figure 4.8: Synchronized measurement test setup

4.6 Summary

In this chapter, a low-cost development and implementation of high-resolution synchronized measurement units for distribution network are presented. The developed unit utilizes a publisher-subscriber peer-to-peer communication scheme to construct synchronized measurement networks. All measurement units are synchronized and measure the phase angle relative to the GPS time reference. The DDS eliminates the need for the phasor data concentrator and provides a reliable communication network.

Chapter 5 Smart Grid Modeling and Simulation

5.1 Introduction

The challenge of maintaining reliable control and operation of the grid with a number of subsystems increases the level of uncertainty, not only on the demand side but also in terms of generation availability. These subsystems integrate a wide variety of resources that are governed by different regulations and owned by different entities. Deep integration between intelligent measurement nodes, communication systems, IT technology, artificial intelligence, power electronics and physical power system components is needed to manage the modern smart grid resources. The dynamic behavior of such a complex system is dependent on a wide range of factors distributed between cyber and physical components. Understanding the dynamic behavior and expected performance of such complex cyber-physical systems (CPS) is challenging.

To study the complete system behavior, a new set of tools for modeling and analysis of the complex cyber-physical system is required. The currently available simulation tools, emulation tools, and test beds focus only on the physical or the cyber part. The expected capabilities of simulation and physical testbeds differ significantly. Simulation is typically used to evaluate the overall system performance in order to obtain the big picture. Physical test-beds, on the other hand, offer the important capability of being able to operate a real system that produces detailed responses. Physical test-beds provide the real operation of the micro-grids, which can be used to evaluate the actual behaviors and impacts of embedded systems, software and physical component on power system operation and stability. Because of resource limitations, however, physical testbeds

cannot represent all elements of the entire large-scale cyber-physical system. Conversely, simulation offers greater flexibility and scalability, but cannot provide the operational realism. A hybrid hardware/software-based smart grid testbed infrastructure [36] is required to represent the interaction of the cyber and physical components to understand the system dynamics and evaluate new designs [35].

The testbed should provide the necessary hardware and software environments to perform different types of experiments, such as HIL, as well as SIL operational control in real-time. Real-time embedded systems have different dynamic behaviors based on processor speed, communication channels, memories and embedded firmware. The modern power system network heavily depends on real-time embedded systems. Components such as PMUS, Protection Relays etc. are examples of critical real-time systems that exist in the modern grid. Hardware in the loop simulation platform is required to evaluate the effect of actual behaviors of these embedded systems in power systems operation and stability. The hardware in the loop platform provides the method of simulating large power system network while at the same time interacting with actual hardware components. Since these hardware components communicate using different protocols, providing a communication interface with interoperability with simulation platforms is challenging. The integration between the proposed co-simulation framework and smart grid testbed will provide a flexible hybrid software/hardware environment for modeling and testing different smart grid operating scenarios.

Since The CPS is a multidisciplinary system, the testbed should provide a standard and flexible interface to integrate with other testbed facilities from different domains for

multidisciplinary studies. This type of integration provides the scalability to represent large cyber-physical systems [61] and enable cooperation between researchers from multidisciplinary fields for a better understanding of different domain interactions.

Several smart grid and CPS testbeds have been developed to represent the cyber-physical interaction in the smart grid. However, none of them provide the tools and interface to integrate several testing platforms into a scalable system that can also be expanded to accommodate new types of services, components, and operation scenarios [62]-[64].

The proposed testbed infrastructure not only allows for integration with other testbeds, but also enables remote experimental features to perform experiments, test developed algorithms, and collect data remotely. Figure 5.1 shows the block diagram for the proposed hybrid smart grid testbed. The testbed consists of three different layers.

The first layer is the physical layer, which represents a scaled model for smart power systems, including generators, transmission lines, circuit breakers, PMU, loads emulators, embedded controllers, and remote terminal units (RTU) for supervisory control and data acquisition (SCADA).

The second layer is the communication layer. The DDS serves as backbone and interoperability layer between all components is the testbed. DDS shares all information, measurements, and control command through a unified global data space (GDS) using a publisher-subscriber communication scheme. Data from different devices and protocols are translated and shared through the developing DDS gateway.

The top layer is the software layer. In this layer, three different types of software modeling and simulation, data visualization, and protocol emulation are integrated with the testbed. The modeling and simulation software is used to model, test, and verify a new control algorithm using HIL technology. After testing the modeled controller, actual implementation code can be verified with real hardware using the SIL simulation technique. The simulation environment can be used to model and simulate large-scale power systems. The simulation model can exchange the information with actual devices, such as PMUs and protection relays, through the communication and interoperability layer. A toolbox is developed to integrate the MATLAB/SIMULINK modeling and simulation software package with smart grid testbed. The developed toolbox is described in the next section.

Data visualization runs a well-designed interface on a user front-end machine for experiment specification, configuration, visualization, control, and analysis. It allows the user to easily specify the experiments, visualize the system configurations, change the model parameters, inspect or modify the system state for the experiments, and allows for on-line monitoring and steering of the experiments. A graphical user interface and online monitoring are developed using LABVIEW. The LABVIEW interface shown in Figure 5.2 allows online monitoring for all measurements and override control command from controllers. The user can also visualize all data of interest in real time using MATLAB graphs and SIMULINK scopes.

Modern smart grid utilizes different types of protocols; the protocol emulation is used to integrate several protocols with the testbed, communicate with real devices or

investigate the security and vulnerability in a safe environment. To investigate the security and vulnerability, virtual IEDs are created on a virtual or embedded platform. Virtual IEDs can communicate with real IEDs using protocol emulation and simulation software using the DDS backbone. Protocol emulation will be described in section 5.3.

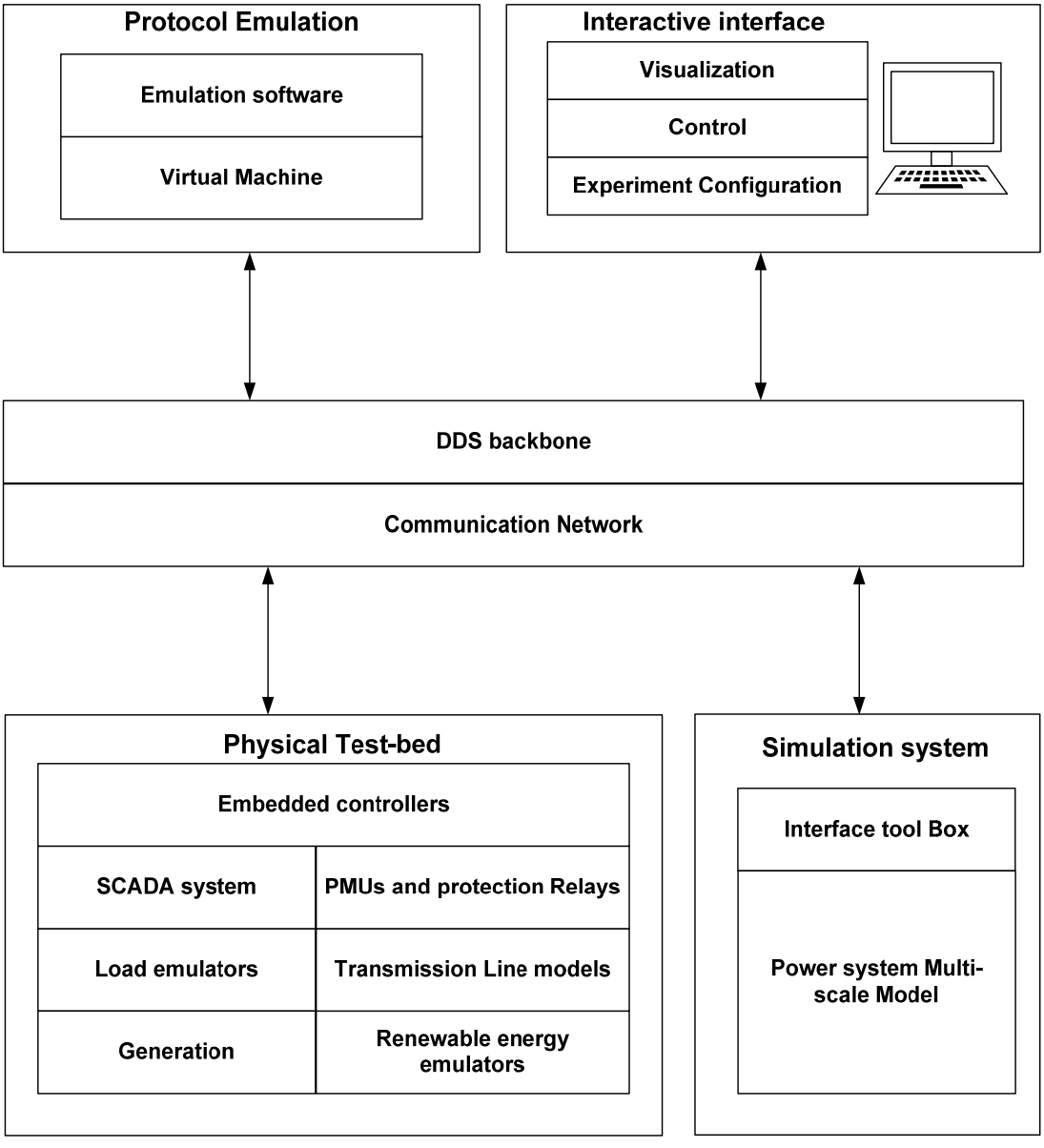


Figure 5.1: Hybrid Smart Grid Testbed Block Diagram

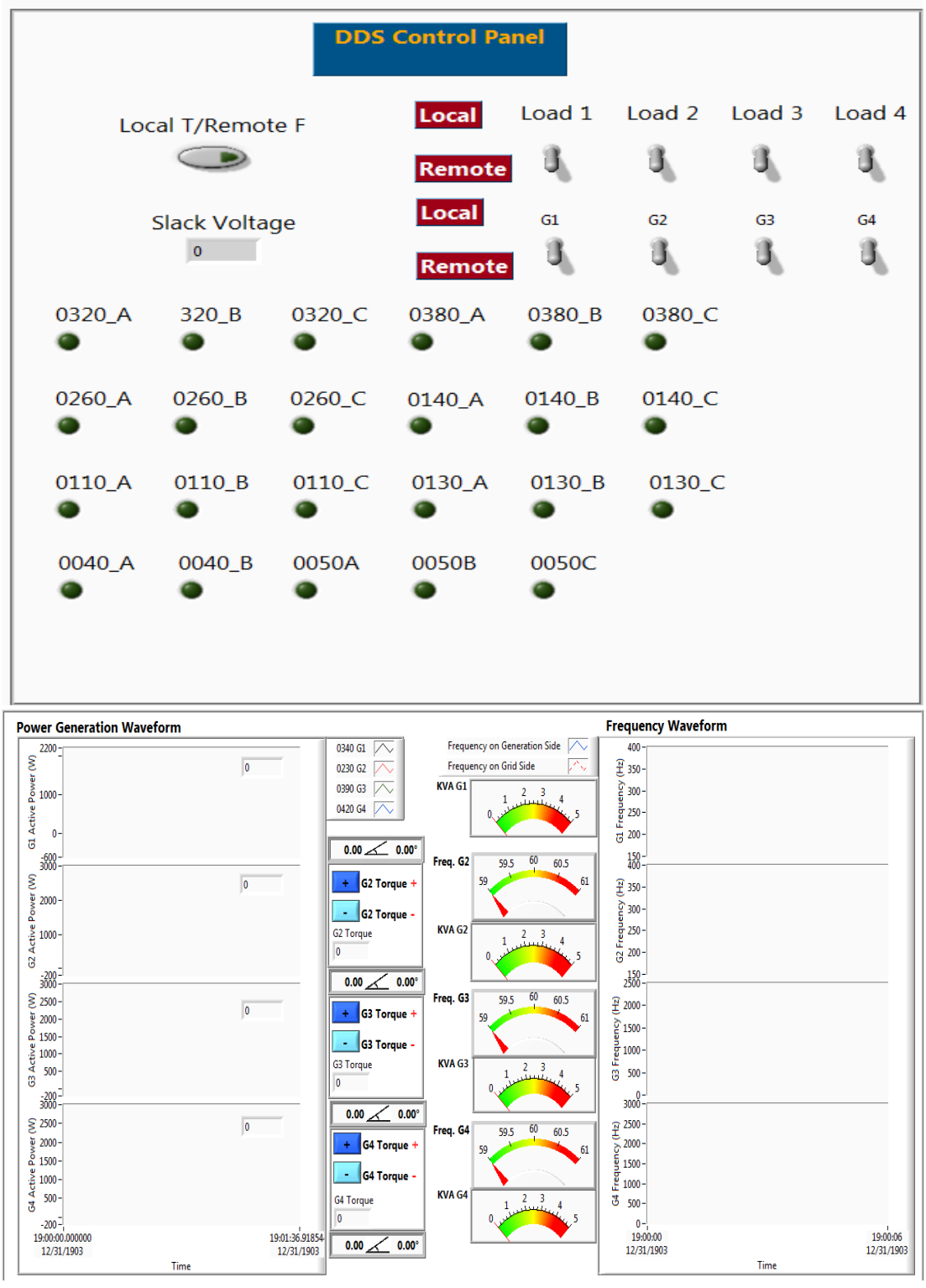


Figure 5.2: Testbed LabVIEW Interface

5.2 Hybrid simulation toolbox

Based on a defined data structure for the testbed objects, a Simulink toolbox was developed to provide an interface between Matlab/Simulink and testbed hardware. The toolbox utilizes the DDS middleware and MATLAB support package to integrate MATLAB, DDS, and physical hardware. This toolbox allows users to perform an experiment, control testbed hardware in real-time and collect data through an Ethernet network. A routing service can be used to allow remote access and experimentation through a high-speed virtual private network (VPN) connection. The main blocks for the main objects of the testbed are defined as the following:

5.2.1 Domain Creator block

The domain creator block shown in Figure 5.3 creates and initiates the domain for the DDS where all the publishers and subscribers share the data in a global data space. Each domain has a unique integer ID number. Simulation objects must join the same domain to communicate to each other. A simulation model can be a part of multiple domains by using multiple domain creators with multiple IDs, as shown in Figure 5.4. The user needs to set the domain ID in the block parameter. The domain creator block has two output ports: Sub port and Pub port. The Sub port should be connected to any simulation object that needs to read data from the GDS. Pub port should be connected to any simulation object that needs to write data to the GDS. Domain can be used to isolate different tests running in the testbed at the same time or group multiple objects which belong to the same system such as two different microgrids. If the domain already exists with the same ID the domain creator participates to the existing domain.

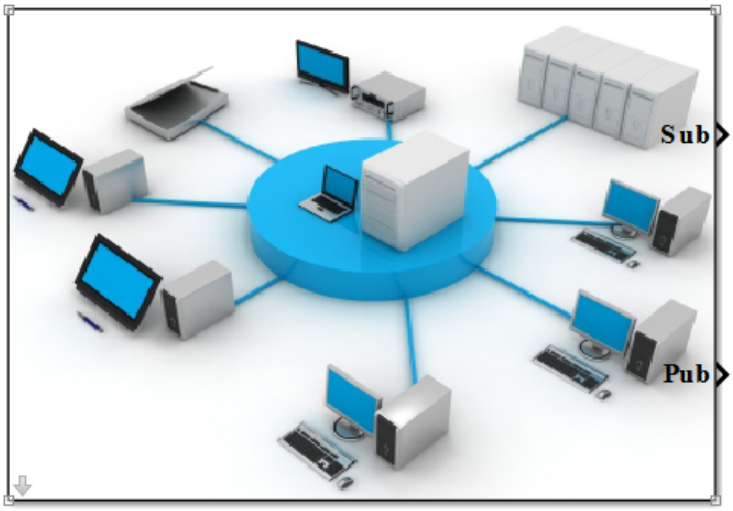


Figure 5.3: Domain Creator.

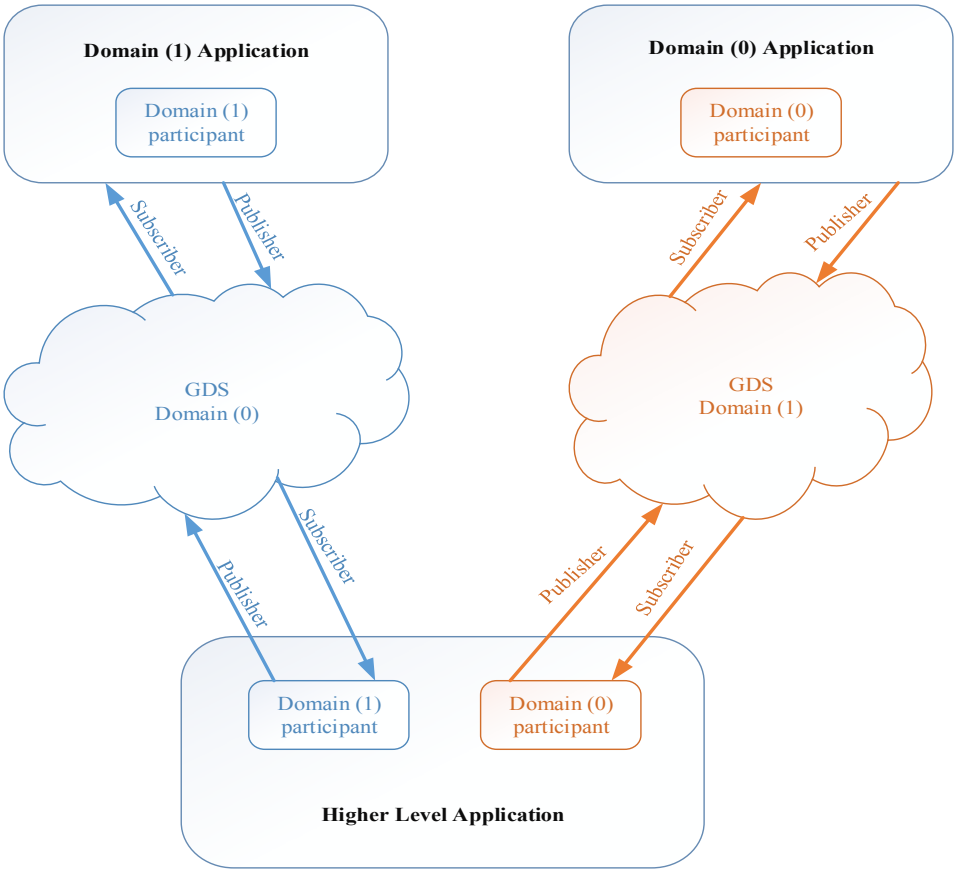


Figure 5.4: Multiple Domain Creators with Multiple IDs

5.2.2 Generator control Block

A control Block was defined for the generators, as shown in Figure 5.5. The generator Block publishes the control command, speed/torque reference, start/stop control and synchronization command to the GDS. The actual measurement of the generator current, voltage, active and reactive power, and frequency are returned to the simulation by subscribing to measurement topics in the GDS. The user can set the QoS profile for an individual topic in the generator block, as shown in Figure 5.6. Each generator block contains two inputs for the publisher and subscriber configuration. These two inputs should be connected to the corresponding outputs of the domain creator block. Two types of generator blocks are defined based on the control mode, either speed control for a slack generator or power control for other generators in the system.

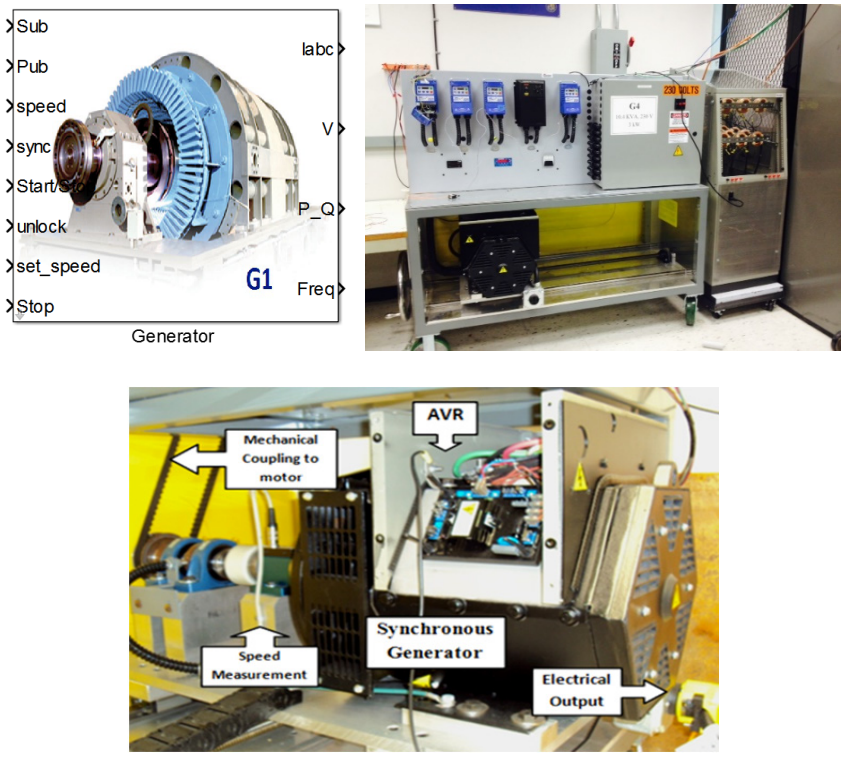


Figure 5.5: Generator Control Block

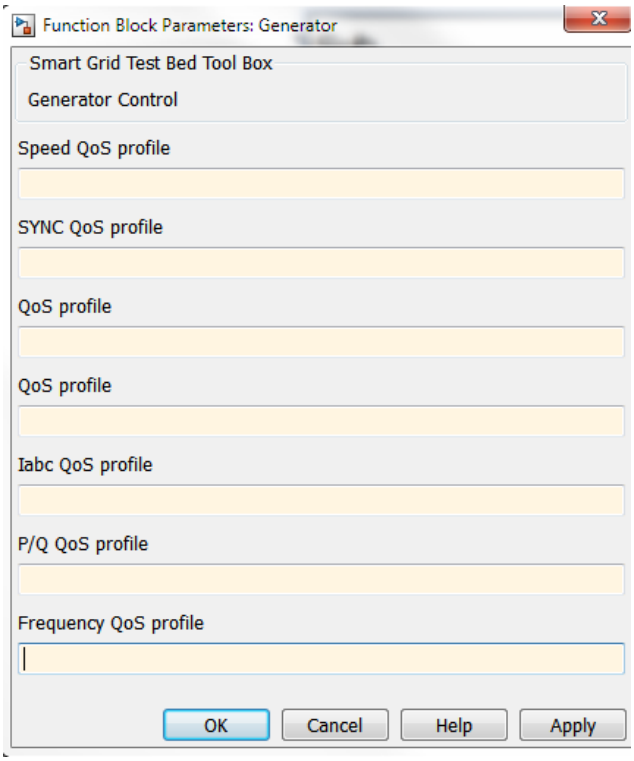


Figure 5.6: Generator Control Block Parameters

The physical generation stations receive the control command through an RS-485 serial interface. In order to pass the data topics from Ethernet-based network to RS-485 serial communication network, an interface board shown in Figure 5.7 is designed.

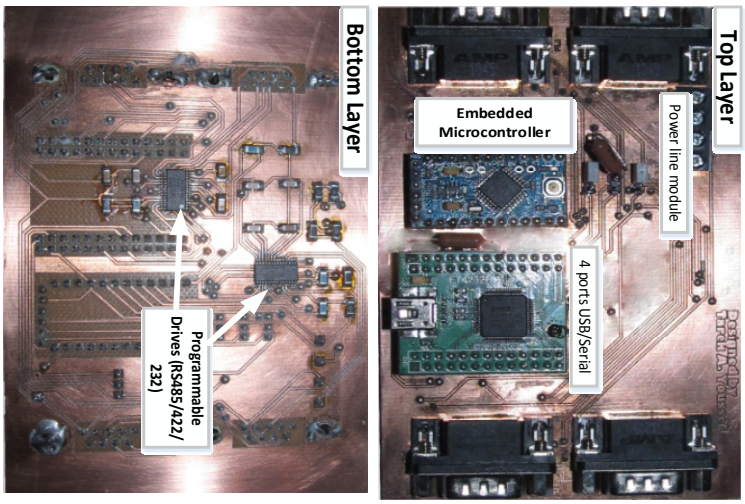


Figure 5.7: Serial Interface Board

The interface board has four programmable serial ports, USB, and a power line communication (PLC) modem port. Each individual serial port can be programmed to work as RS-485, RS-422 or RS-232. Three serial ports can be accessed directly from a computer or an embedded host using a USB communication device class driver (CDC). The fourth serial port can be configured as a PLC port or regular serial, as shown in Figure 5.8.

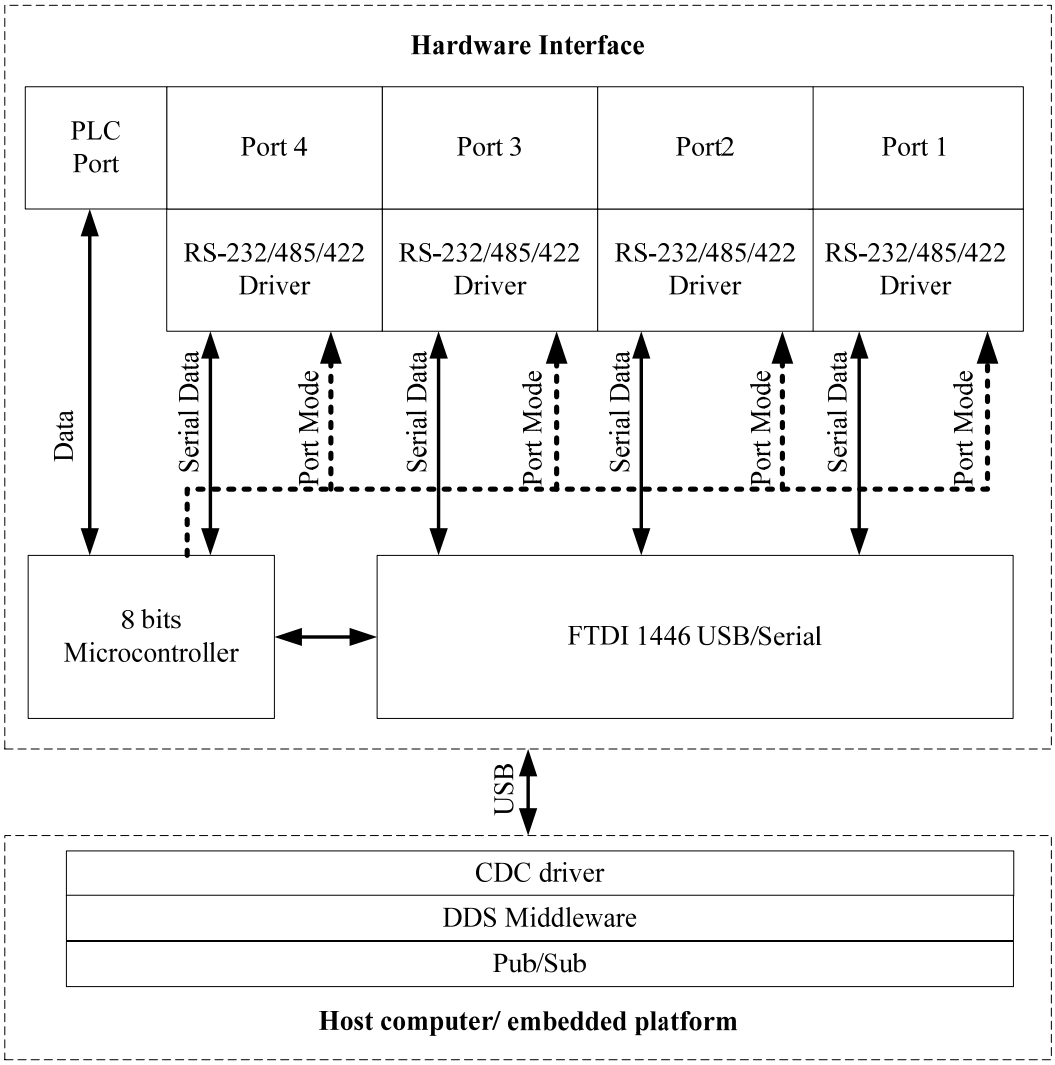


Figure 5.8: Interface Board Block Diagram

In the case of PLC port configuration, the built-in microcontroller performs the hard-real-time tasks for power line communication in addition to controlling serial ports modes. The Microcontroller Firmware can be updated over USB communication. The same interface board can be used to pass the data from PMU C37.118 serial protocol to the DDS global data space.

A. Circuit Breaker

The block controlling the CB is shown in Figure 5.9. This block receives the CB control signal and controls the actual CB. The user can set the QoS for the control signal, as shown in Generator's control block.

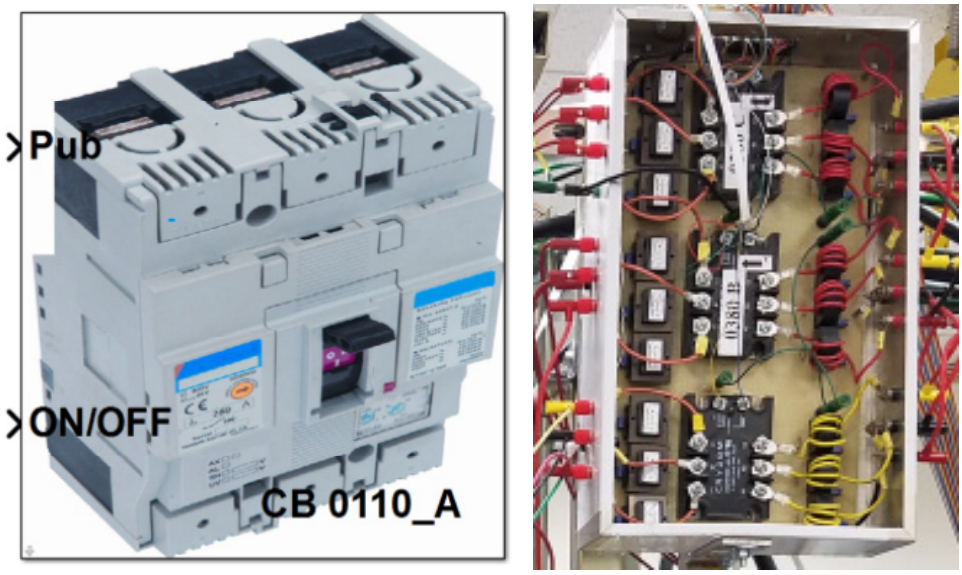


Figure 5.9: Circuit Breaker Block Diagram

B. Load

Four different programmable loads are controlled by the load control block in Figure 5.10. Load controllers can control active and reactive power for each load to represent load patterns. The control block must be connected to Domain creator Pub port.

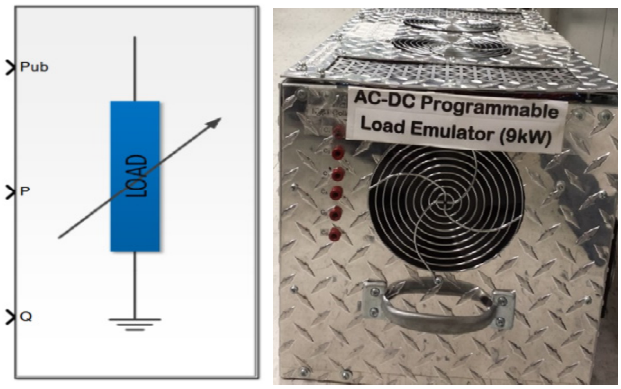


Figure 5.10: Load Control Block

C. Busbar

The Busbar block is shown in Figure 5.11 monitors the three phase voltage for the Busbar of interest. The user can choose the Busbar number and assign the QoS profile for the measurement data.

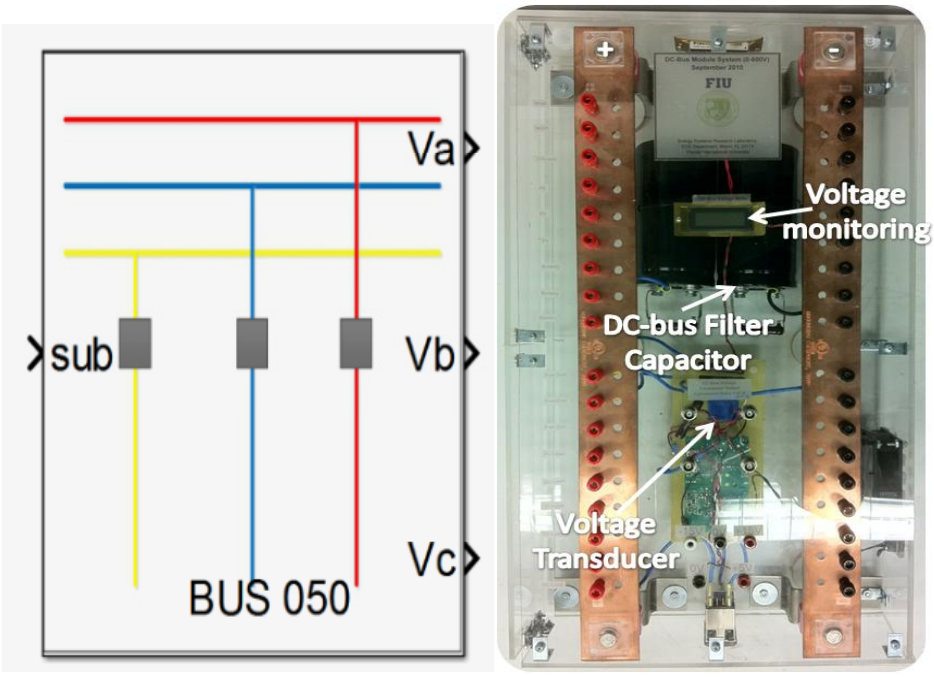


Figure 5.11: Busbar Block

D. Transmission Line

The transmission line block depicted in Figure 5.12 is used to monitor the transmission line current. The block has one input port for subscriber connection and three output ports for three phase current output. The user can choose the transmission line and QoS profile from Block parameter.

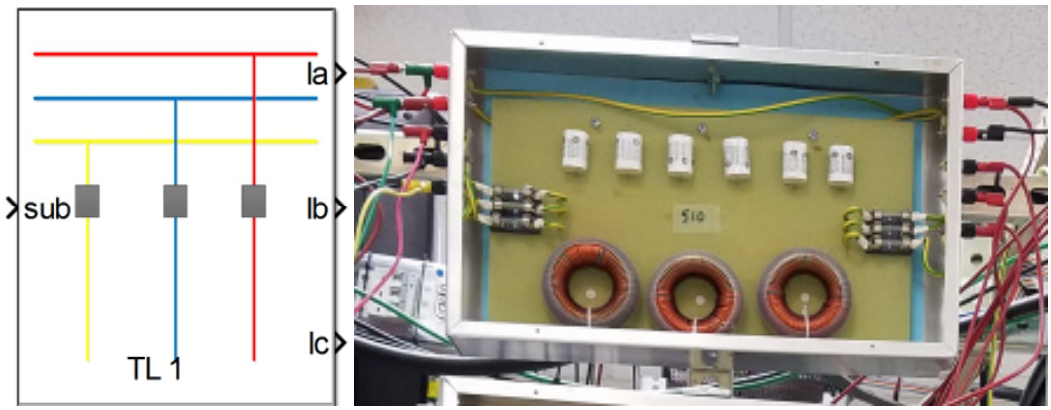


Figure 5.12: Transmission Line Block

E. Microgrid

An inverter based hybrid microgrid can be controlled from the simulation environment using the developed toolbox. The hybrid microgrid showed in Figure 5.13 consists of PV emulator and wind turbine emulator connected to a common DC bus. The energy is transferred from the DC side to AC side or vice versa through a bidirectional power electronics converter. The microgrid can work in two different modes, grid-connected, and islanding mode. In grid-connected mode, the converter is controlled to regulate the current injected to the utility. The microgrid controller receives a reference for active and reactive power and regulates the current to inject the required energy amount to the main grid. In islanding mode, the microgrid controller regulates the output voltage of the power electronics converter to maintain constant AC voltage at the load

terminal. The microgrid is represented in the Toolbox by the control block shown in Figure 5.14. The control block has several inputs to control the microgrid's operation mode, voltage, power and reactive power references. Furthermore, it reads all the AC and DC voltage and current measurements from the hardware. The microgrid control algorithm is running by the real-time embedded controller dSPACE DS11013. The data are exchanged between the host computer and the controller using the developed serial interface board.

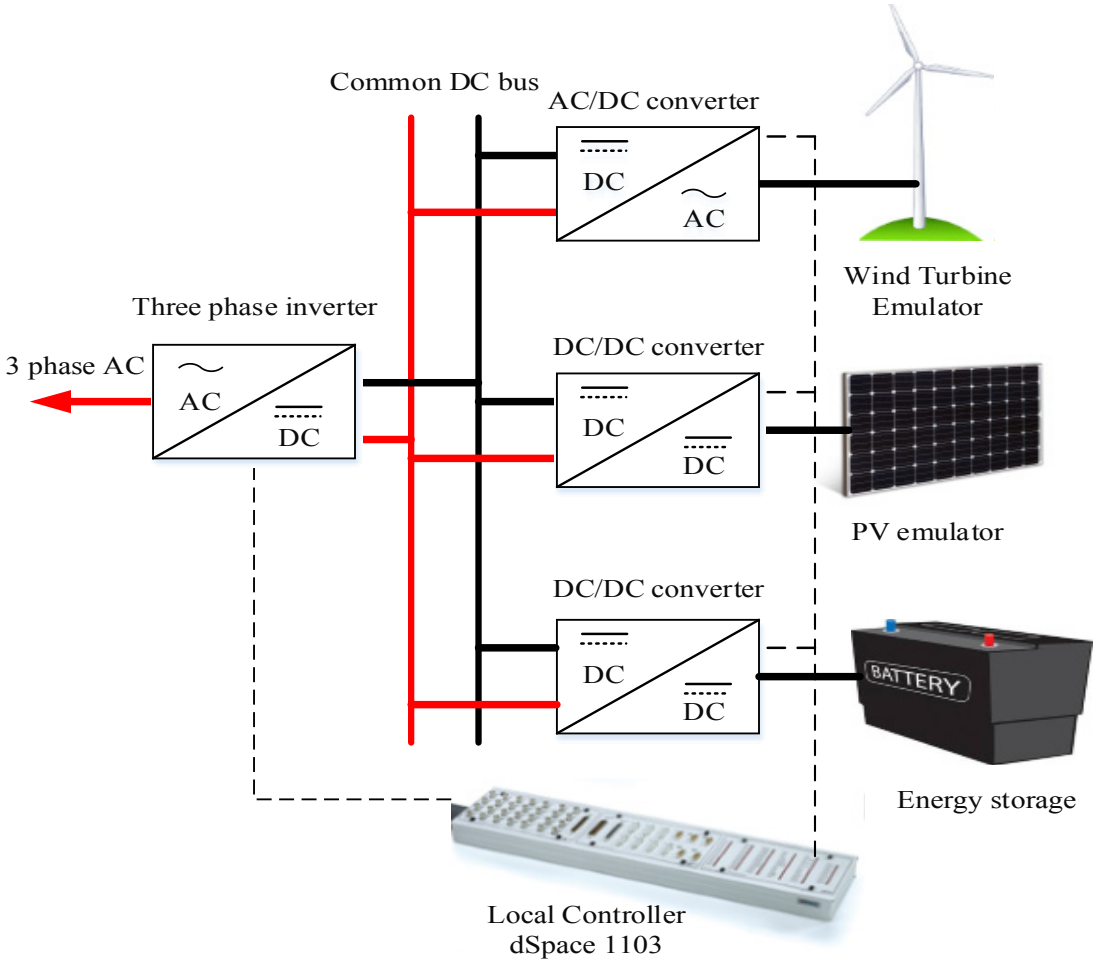


Figure 5.13: Hybrid Microgrid Block Diagram

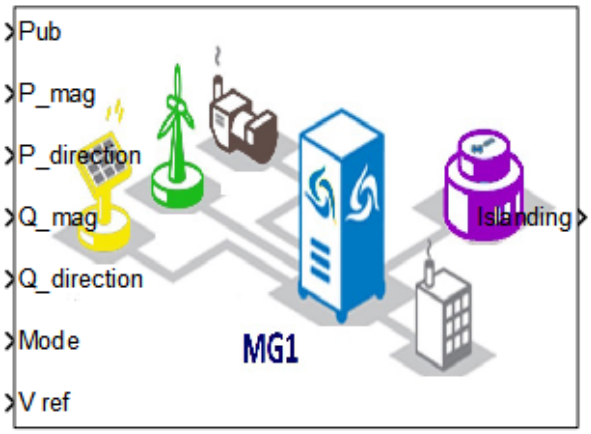


Figure 5.14: Microgrid Control Block

F. Smart Meter

The smart meter block is shown in Figure 5.15. This block receives the total accumulated active and reactive power consumption from the physical smart meter over the last hour, as well as power consumption every minute. In addition, it receives the RMS values for voltages and currents.

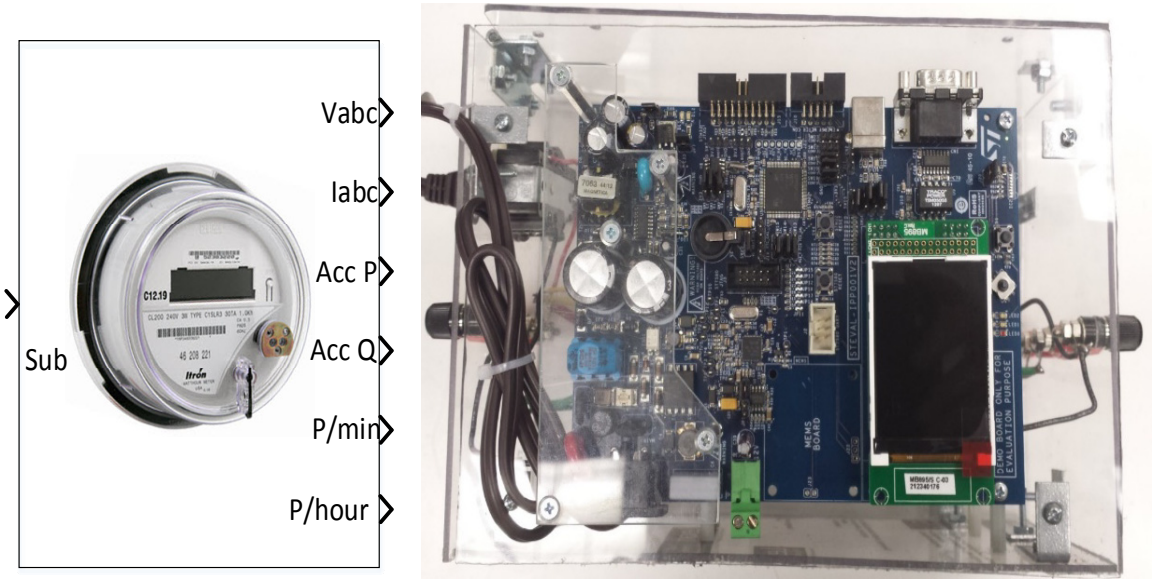


Figure 5.15: Smart Meter Block

G. Energy Storage

The physical energy storage is controlled through the block shown in Figure 5.16. This block receives the voltage and current measurements and the calculated State of Charge (SoC) from the energy storage controller. In addition, it sends a current reference to control the charging and discharging of the energy storage array. Some types of energy storage, such as lithium-ion, are temperature sensitive. Thus, this block is flexible for additions, as other parameters can be added depending on the energy storage type.

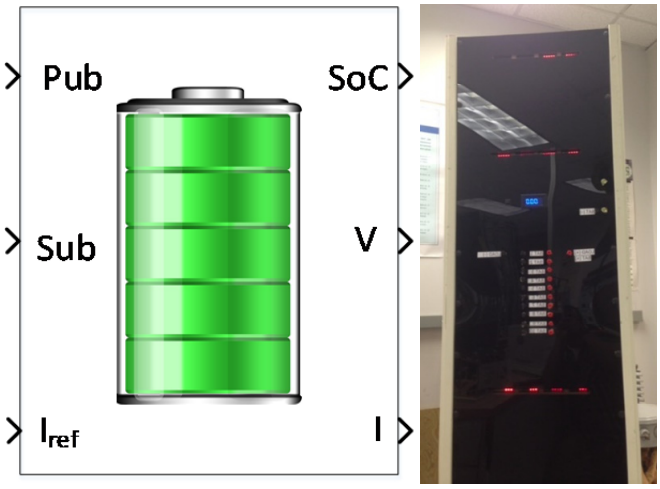


Figure 5.16: Energy Storage Control Block

H. Database Service

A real-time subscriber service can be configured to monitor the data from the GDS and store it in a database server for later analysis, as well as publish stored data from the database server. This data can represent a real load, solar irradiance, or a wind speed pattern. The publisher-subscriber configuration defines the data rate, object, topic name, and data tables. The integration with the database server simplifies the data logging during experiments and utilizes historically collected data for testing new algorithms.

Each block in the toolbox allows defining a QoS profile individually for each topic. The settings for QoS profiles are defined in an XML file. Preset QoS profiles were created to provide the necessary QoS settings for each type of data. The QoS profile for CB signals is configured to provide the minimum possible latency with a durability option set to store and deliver the data to a late or newly created subscriber. This setting ensures the delivery of a CB control signal and correct initializations when joining the network, even if the subscriber created it after transmitting the control command. For measurement signals, each sample is time-stamped two times. The first time is stamped by the sender at the transmission instant and then stamped at the receiver at the receiving instant. To ensure synchronization and a correct order of samples, the QoS profile for measurement signals were set to deliver the data ordered by the sender timestamp.

The implementation of the HIL is depicted in Figure 5.17. It can be seen that the control algorithm is simulated in the Matlab/Simulink environment. The control command is transmitted to the real hardware using the developed interface toolbox over the network using the DDS middleware and specified QoS. Real-time feedback from the physical measurement points is transmitted back to the Simulink model. The generator block in the HIL model replaces the regular Simulink simulation model for a synchronous machine with the actual machine. This capability makes it possible to consider the real behavior and dynamics of the physical system in control design. In addition, the HIL model represents the system as an integrated CPS by taking into account the effect of the communication network behavior. The impact of different communication topologies and QoS profiles on the performance of the system can be investigated.

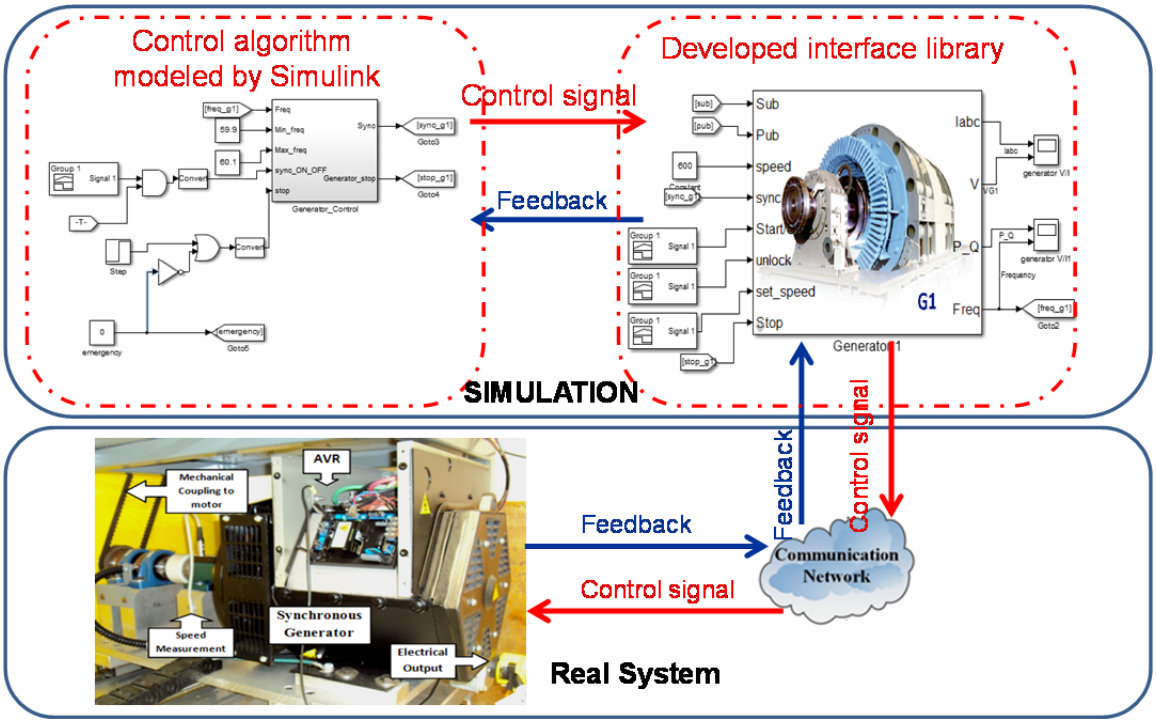


Figure 5.17: HIL implementation using DDS and the developed interface library

To simplify the initialization and startup of the testbed, an automated startup and initialization procedure was developed using a state machine. These startup and automation controllers abstract the procedure of initializing the testbed physical components by performing all the necessary steps to run the testbed. The startup controllers set up the system frequency, startup and synchronize the generators, configure the network topology, and connect the different loads. The shutdown procedure ensures a correct shutdown sequence to prevent component damage. The user can utilize this controller as it is or use it as a base template to build his own controller. The hierarchy of the automatic controller is shown in Figure 5.18, where it can be seen that the control is divided into two levels. The low level consists mainly of three state machine controllers. The state machine for the first controller is shown in Figure 5.19, which is responsible for

starting up and shutting down the slack generator. In the startup state, the controller sets the speed of the generator at the required value depending on the required operating frequency. Then, it changes the status of the generator to the "on" state. When the output voltage and frequency reach the nominal values, the controller generates a ready signal to indicate that the slack generator is ready. While the slack generator is in a shutdown state, the controller sends a turn-off signal to the generator and resets the generator ready signal to zero. Figure 5.20 shows a connection example of the slack generator and state machine controller.

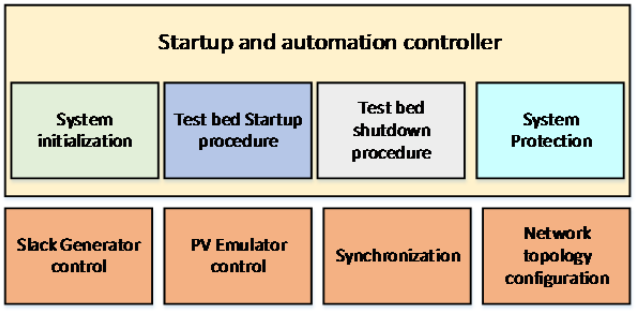


Figure 5.18: The hierarchy of the developed automatic controller for the smart grid testbed

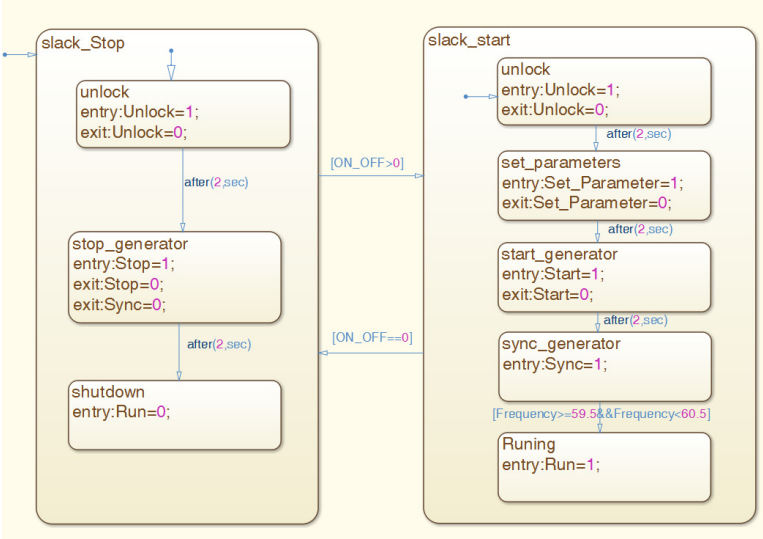


Figure 5.19: Slack generator control

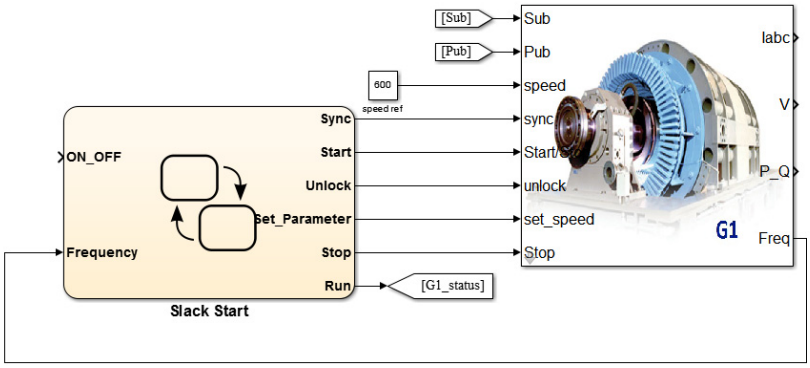


Figure 5.20: Slack generator control connection

The state machine for the second controller shown in Figure 5.22 is responsible for the startup/shutting down of the power controlled generators in the system. In the startup state, the first step is to send a start signal to the generator, then start the synchronization process shown in Figure 5.21. After the synchronization process has completed, the controller closes the generator CB to connect the generator to the testbed. After that, it generates a ready signal to indicate the successful completeness of the starting-up process. In the shutting down state, the controller opens the generator CB and sends a shutdown signal to the generator. Figure 5.23 shows a connection example of the PQ generator and a state machine controller.

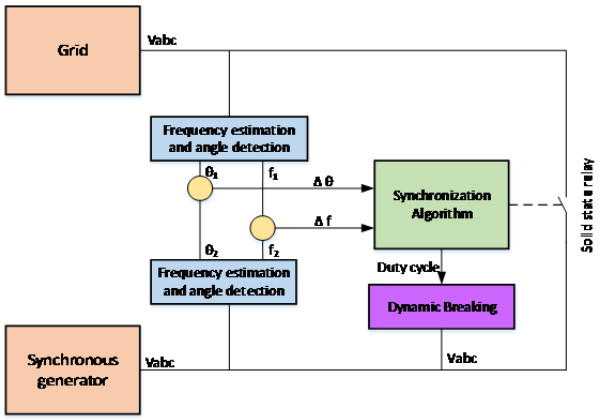


Figure 5.21: Synchronization Controller

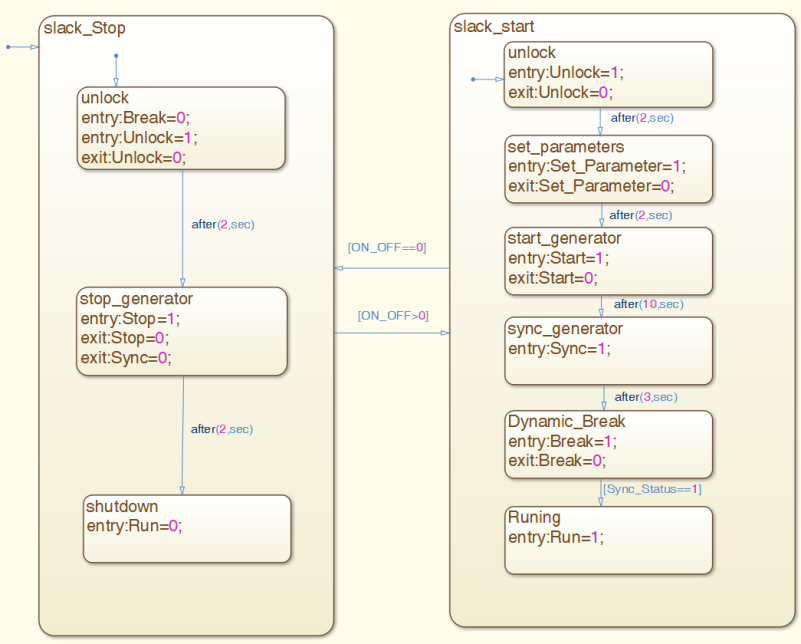


Figure 5.22: Power controlled generator control

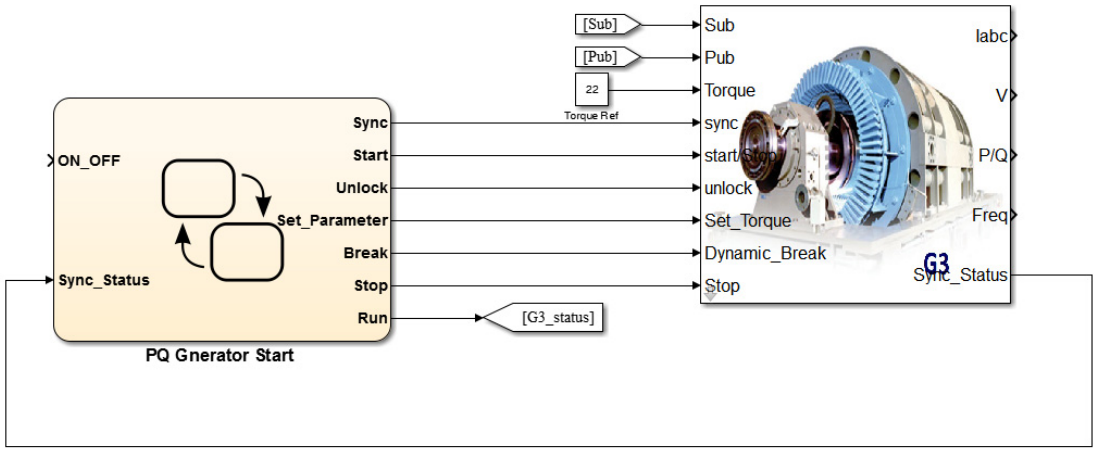


Figure 5.23: PQ generator controller connection.

The high-level controller is responsible for coordinating the operation of the low-level generator startup controllers and configuring the testbed network topology by connecting necessary transmission lines, busbars, and loads. As shown in Figure 5.24, the main controller consists of two main states: namely, startup and shutdown. In the startup

state, the controller calls the generator startup algorithms in the required order and monitors the generator status. Then, it connects the CBs to configure the testbed topology and connect the loads. Once all the generators are running and the topology configuration is done, it generates a ready signal for the entire testbed. This signal can be used to enable starting up a certain experimentation procedure. In the shutdown state, the controller shuts down the generators in the correct order by shutting down the power controlled generators one-by-one while disconnecting any connected loads to avoid overloading the remaining generators. Finally, after shutting down all the power controlled generators, the slack generator is disconnected and all circuit statuses are reset to an open state.

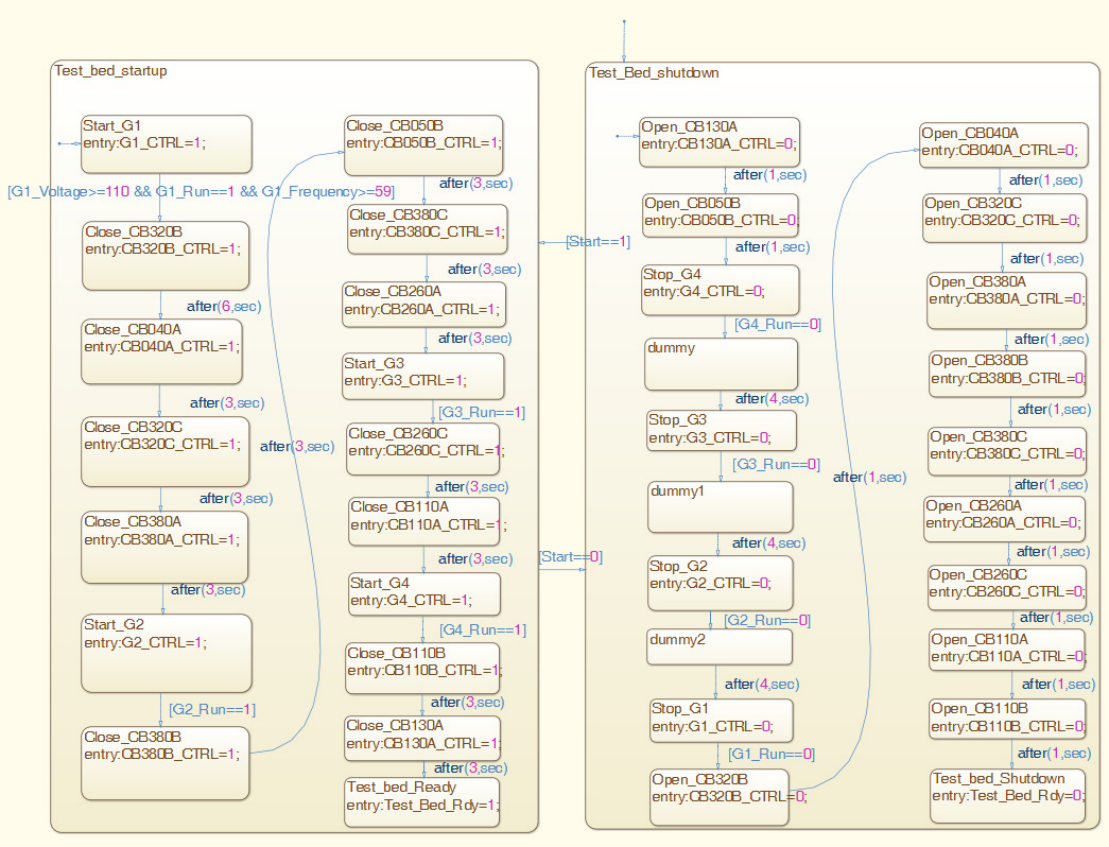


Figure 5.24: Main automation and startup controller

5.3 Protocol Emulation

A software layer running in a virtual environment or an embedded host is used to emulate standard communications protocols utilized in power system operation. The emulation layer allows interaction between the simulation environment and commercial IEDs, such as protection relays and PMUs. The interaction between simulation and actual IEDs is necessary for testing new algorithms and the performance of actual devices with different firmware versions in a safe environment. The emulation layer consists of a number of virtual IEDs that communicate with real IEDs with emulated protocols and maps all data to the DDS global data space. Figure 5.25 show the block diagram for emulating IEC 61850. The emulation process is done through three layers, the first layer is the real IEC 61850 devices connected to an Ethernet-based network.

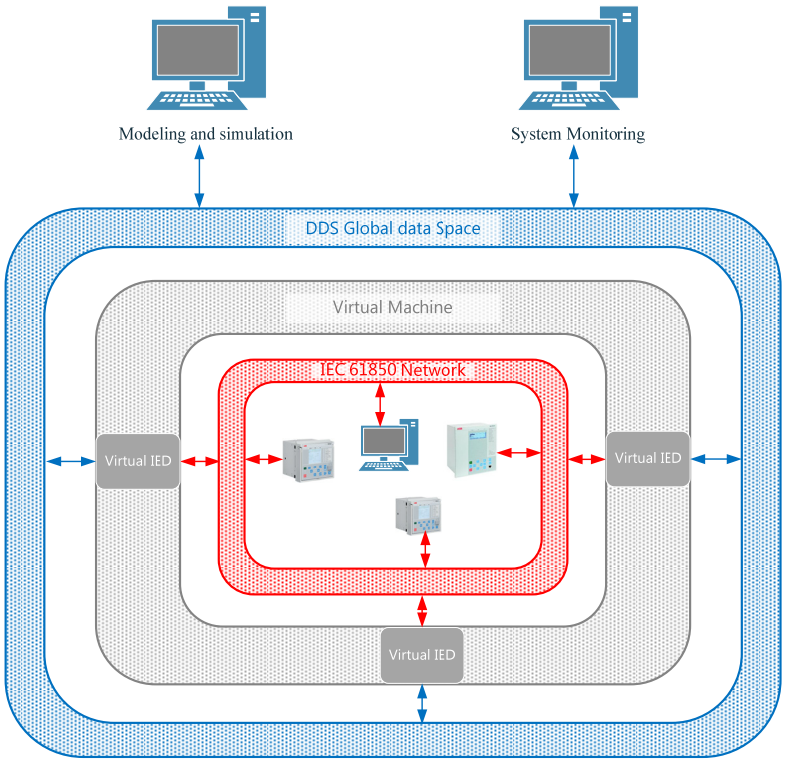


Figure 5.25: Block Diagram for IEC 61850

The second layer is the virtual IEC61850 devices running in a virtual environment and connected to the same Ethernet network. Virtual IEDs represent a bridge between the IEC61850 network and DDS global data space by receiving different types of messages and mapping them to DDS data topics and vice versa. The third layer is the DDS backbone in which all data topics are shared with the simulation environment and system monitoring.

To create a virtual IED, the data model for the device should be defined, then emulation code for the IEC 61850 and DDS publisher/subscriber functions is generated, as shown in Figure 5.26.

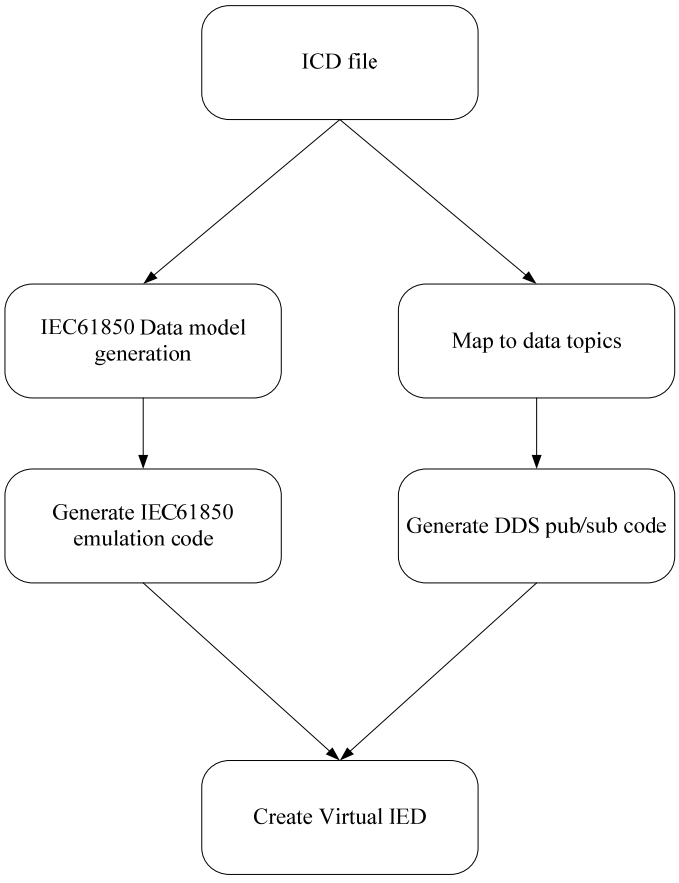


Figure 5.26: IEC 61850 and DDS publisher/subscriber functions

The data model can be generated from IED Capability Description (ICD) file. The ICD file is supplied by the manufacturer or can be generated using the automatic discovery feature. Once the device data model is obtained, it can be mapped to DDS data topics and generate a pub/sub C code. Pub/sub code is generated using automatic code generation supported by the RTI DDS library. The IEC61850 emulation code is created based on the libiec61850 open source library. Libiec61850 provides open source implementation for different types of IEC-61850 messages, such as MMS, Generic GOOSE and Sampled Measured Values (SMV). The API of libIEC61850 gives the user full control to modify message data field while preventing modification of other fields, such as timestamp, Sequence number, and status number. In regular cases, the user doesn't need to modify those fields. The timestamp and sequence number fields are automatically generated by the Library based on current system time and previous message sequence number. For testing vulnerability analysis, the user needs to have full access to modify and override any message field value. The library is modified to allow this type of modification. The modified library will be utilized for protocol vulnerability analysis and implementation of a security solution for GOOSE message in the next chapters.

After generating IEC61850 emulation code and DDS pub/sub code, both codes are merged and compiled to an executable application. The final virtual IED code is compiled using the GNU C compiler and is run under a LINUX OS.

5.4 Remote connection and Micro Grid Intercommunication

The developed testbed toolbox can be used to access the testbed resources and perform experiment remotely. A remote user can test a new algorithm, collect data and exchange information between different systems located at the testbed and remote location. Figure 5.27 shows the complete configuration for the testbed with remote connection capability. To connect to the testbed, a VPN connection is established over a WAN or the internet. Once the connection is established, the remote user can use the developed toolbox to interact with the testbed resources through the DDS global data space.

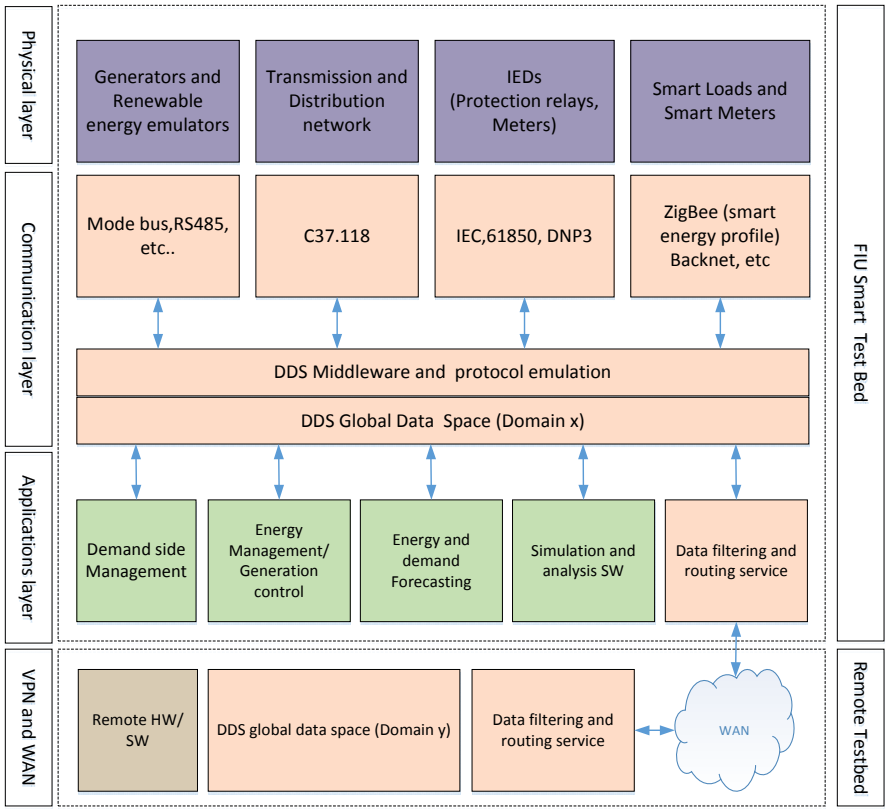


Figure 5.27: complete configuration for the testbed with remote connection capability

To control the data flow between testbed and remote sites and ensure system security, four different domains are created, as shown in

Figure 5.28. The data exchange between the different domains is controlled by a routing service, data filtering, and the Resource Management and Protection (RMP) module.

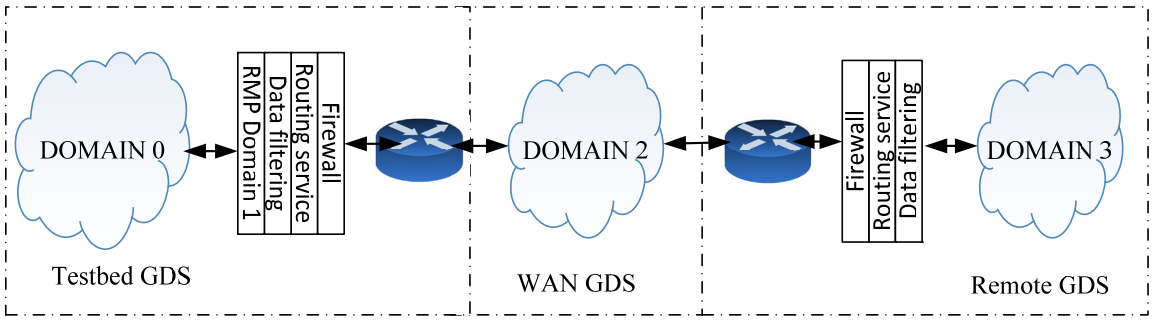


Figure 5.28: Testbed remote access domains

Domain (0) is the GDS domain for the testbed. All the data and control commands generated by testbed equipment are available in this domain. External data from the other domain can be passed to Domain (0) only through the RMP module. The RMP module performs two functions. First, it ensures the remote user only has access to allowed resources. The testbed operator can select which resources are allowed to be accessed remotely. Second, the RMP checks all incoming signals against predefined physical rules to prevent system damage due to a wrong control signal from the remote user. For example, if the testbed operator allows a remote user to control certain generators, connecting non-synchronized generators by mistake to an energized bus could damage the generators. To prevent this damage the RMP will not pass the control signal to close the generator circuit breaker unless the synchronization status is true. In order to perform RMP functions, an intermediate domain is created, Domain (1), as shown in Figure 5.29.

All data coming from the routing service is published first to the intermediate domain. The intermediate domain is a memory shared domain used to exchange information between the routing service and the RMP located on the same machine. Only applications physically located on the same machine can access the memory shared domain. RMP checks all received data against permission and-and physical rules. When the permission and physical rules are matched, the RMP enables the publisher and subscriber to the testbed domain (Domain 0).

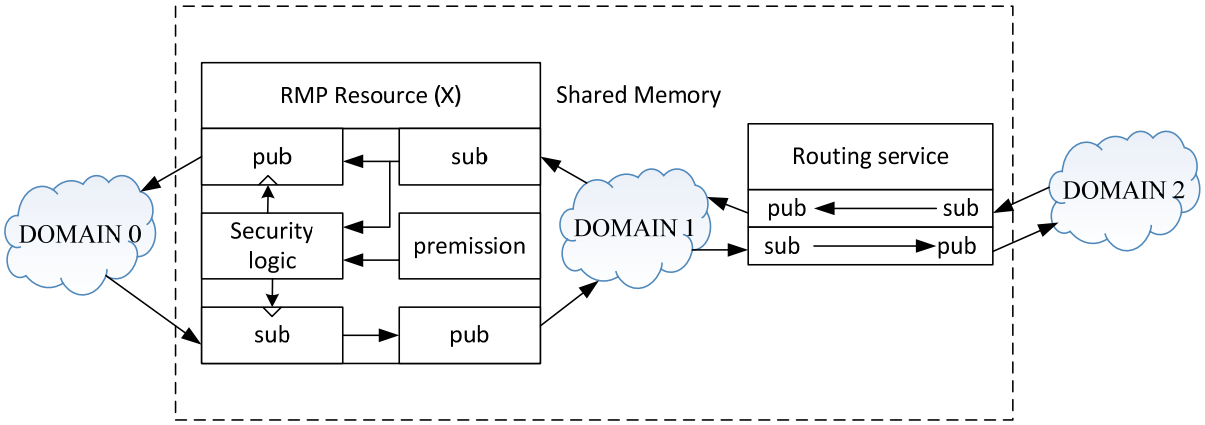


Figure 5.29 Routing service intermediate domain

The routing service is used to route the DDS TCP and UDP communication between two different domains over WAN using only TCP communication. Only data with a remote subscriber are routed over the WAN connection. The routing service allows applying data filtering for data transmitted over WAN. A remote user may be interested in the certain type of data when it matches a certain condition. An example is a protection system interested in current measurements when the current magnitude is greater than certain limits. If the data filter is applied, the current subscriber will not receive any data until the current magnitude reaches the defined threshold. The remote site routing service exchanges the data between WAN domain, Domain (2), and remote site domain, Domain

(3). Unicast and multicast communication can be used in Domain (0), Domain (1), and Domain (3). Domain (2) is a unicast domain only. The remote VPN connection is protected by a password. Transport Layer Security (TLS) can also be used to encrypt the data over WAN. The firewall allows only TCP communication over specified ports used by the routing service. All other ports are blocked.

5.5 Experimental Results

The functionality of the developed communication infrastructure, controllers, and the remote interface toolbox was verified experimentally on the smart grid testbed. For the testbed layout, please refer to Figure 2.5. In order to show the capabilities of the developed framework, three experiments were carried out with different operation scenarios and scales. The first case shows the synchronization process for multiple generators in detail. The second case depicts the load sharing amongst four generators, while the third one shows how the developed framework is used for topology reconfiguration.

5.5.1 Case 1: Generator Synchronization

In this experiment, the capability of implementing a closed-loop high-speed controller using the proposed framework is shown. The synchronization process requires a high sampling rate for frequency and phase angle estimation and low latency feedback. The sequence of automatic system operation starts by starting generator 1 (slack), as shown in Figure 5.24. During this step, a starting signal is sent to the prime mover along with the frequency reference value. The generators' prime movers are controlled using the RS-485 protocol. The protocol translator, shown in Figure 2.8, is used to provide interoperability

between the DDS network and serial protocols. When the slack generator frequency reaches 60 Hz, the automation controller connects transmission lines TL 1-2 and TL 1-8 and then connects load 1. In this scenario, load 1 is set at 600 W. Then, generator 2 is started and synchronized to the slack generator.

The results of the carried out experiments are depicted in Figure 5.30 and

Figure 5.31. Figure 5.30a shows the generator 1 frequency at time 4 s when the startup signal is sent to generator 1. The frequency ramps up until a frequency of 60 Hz is reached. The frequency measured before the generator startup is noise because of the lack of a generator output voltage. At time 9 s, generator 1 is connected and the voltage is stabilized around 115 V, as shown in Figure 5.30d. The load is connected at time 16s, as shown in Figure 5.30e. Figure 5.30b shows the generator 2 startup at time 34 s. It is worth mentioning that the generator 2 frequency was shown as 60 Hz even before the generator startup due to leakage across the solid state switches. This leads to reading a frequency of generator 1 when generator 2 is not connected. Figure 5.30c shows the phase angle difference between generator 1 and 2 voltages. Frequency fluctuations can be seen before the synchronization, but these fluctuations go to zero as soon as the process completes.

Figure 5.31 shows a zoom in on time frame 130–250 s to further illustrate the synchronization process. It is clear that the framework successfully performs an accurate synchronization and frequency stabilization in real-time. Figure 5.30e shows that the slack generator fed all the load while, after synchronization, the load is shared between the two generators.

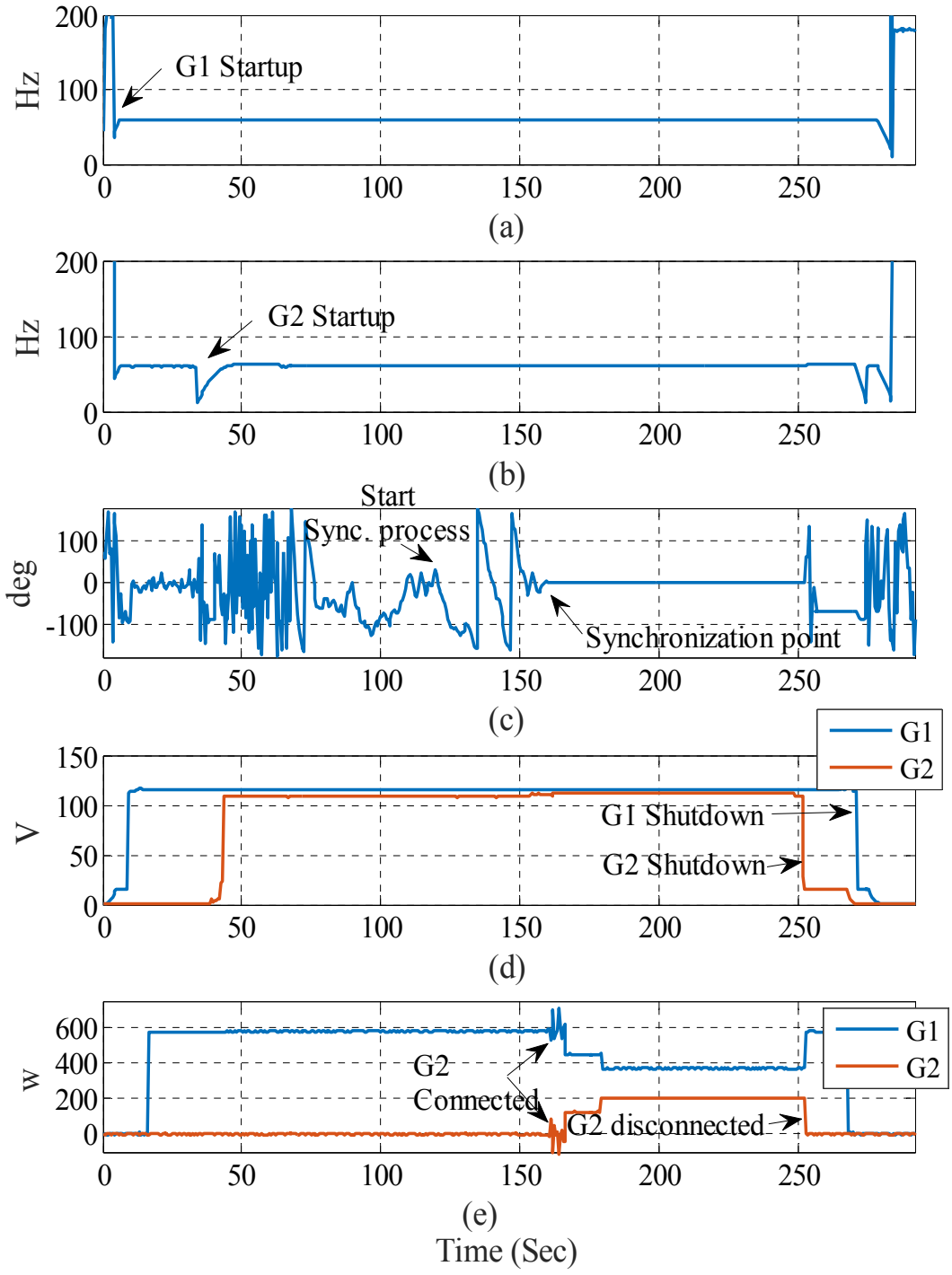


Figure 5.30: Experimental results, voltage, frequency and synchronization switch status (a) Generator 1 frequency; (b) Generator 2 frequency; (c) Generators Voltage; and (d) Generators Power

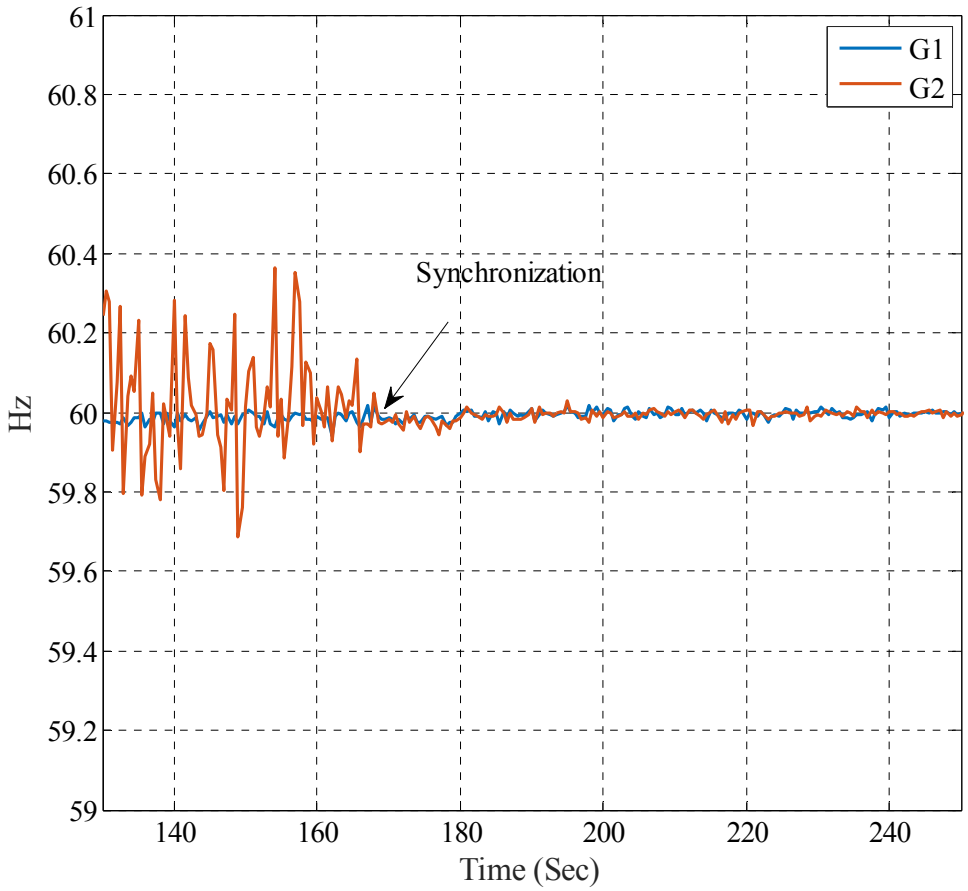


Figure 5.31: Synchronization Process

5.5.2 Case 2: Load Sharing

This case shows the scalability of the developed framework, since four generators, six transmission lines, and two loads are involved. The main focus of this case is to configure the required network topology and control power flow to share the load amongst different sources automatically. The experiment starts by starting generator 1 and connecting it to the load bus through TL 1-8 and to the generator 2 bus through TL 1-2. After that, generator 2 is started and synchronized to the slack generator. Generator 2 is then

connected to the network through transmission lines (TL 2-5). Similarly, generators 3 and 4 are started and synchronized. Then, TL 5-6 and TL 1-6 are connected. The entire startup process is handled by the developed startup and automation controller. During the experiment, loads 2 and 4 were disconnected. Generators 2 and 3 were working in the power control mode with a reference power of 300W. Generator 4 was synchronized and running under no load to represent a spinning reserve. Load 3 was fixed to a value of 300 W while load 1 was varying to emulate a certain load pattern. The control command to the loads was sent over a wireless link. The maximum output power of generator 1 was set to 700 W.

The results of the carried-out test are shown in Figure 18, where the total demand (load 1 + load 3) is shown in Figure 5.32a. The output of the four generators (1–4) is shown in Figure 5.32b–e, respectively. When the total demand changes from 900 W to 1200 W at time equal 65 s, the slack generator output changes from 300 W to 600 W, while the rest of the load is supplied by generators 2 and 3. At time 115 s, the load increased to 1500 W and consequently, the slack generator output is increased to 900 W, which exceeds the preset maximum limit. The controller commands generator 4 to inject power to reduce the slack generator power below the limit. At time 215 s, the load demand decreased to 900 W. In this case, due to low demand, generator 4 returns to reserve mode. An intentional outage of generator 3 is created at time 293 s, where the slack generator output is increased to compensate for the lost generation power. However, the slack generator output is still below the critical limit, hence the controller did not initiate a power injection from generator 4. For this scenario, it can be seen that

the developed framework was able to efficiently exchange data from multiple sources and controllers in real-time to maintain a power balance between load and generation.

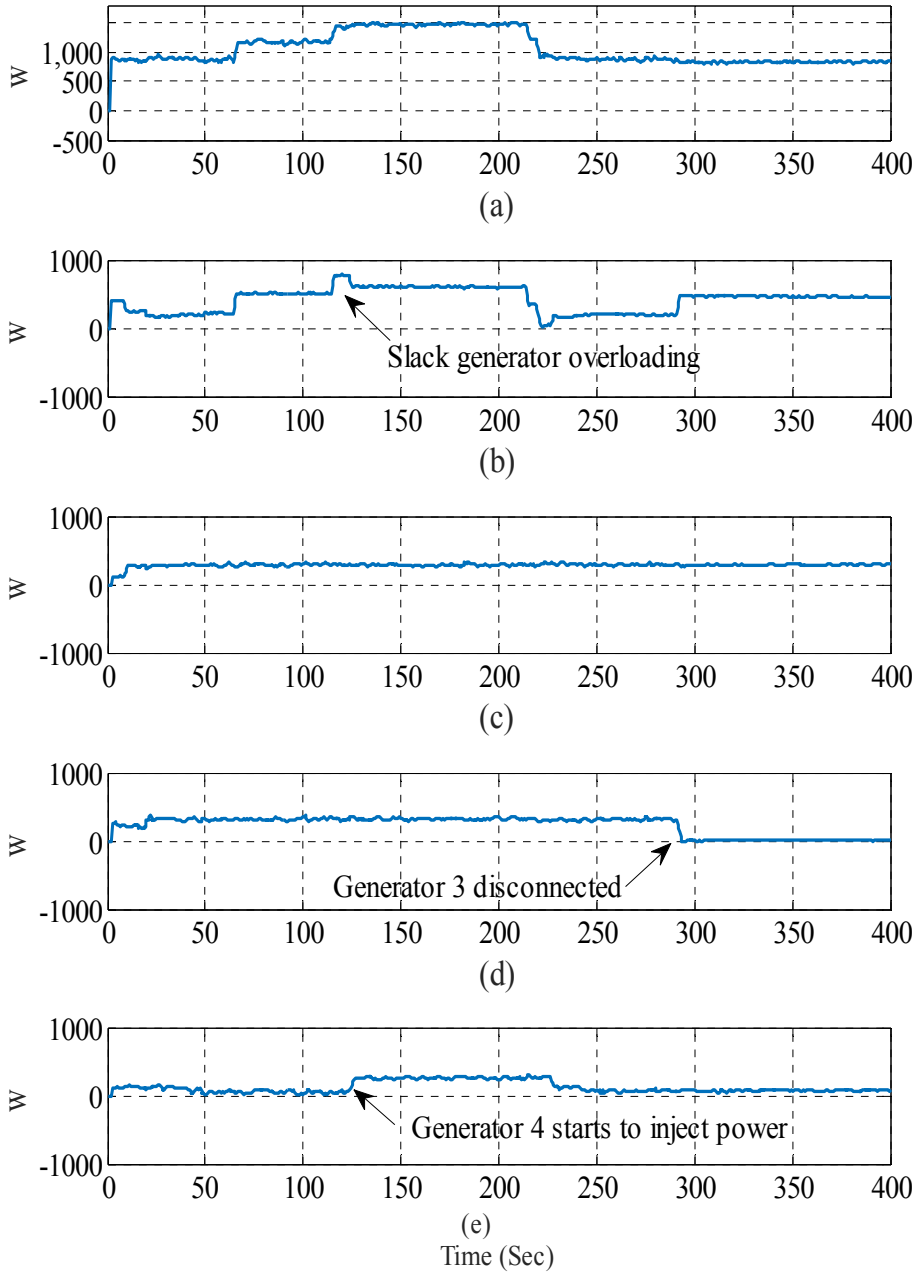


Figure 5.32: Case 2, load sharing. Power of (a) load; (b) generator 1; (c) generator 2; (d) generator 3; and (e) generator 4

5.5.3 Case 3: Topology Reconfiguration

This experiment shows the capability of dynamic reconfiguration of the physical network topology. For this purpose, the radial power transmission network consists of generators 1 and 2, transmission lines TL 1-2, TL 2-5, TL 4-5, TL 5-6, and TL 6-7 and loads 3 and 4 (refer to Figure 1 for the network topology). During high demand, the network topology will be reconfigured to a ring by connecting TL 1-6 to improve the voltage profile. During this experiment, load 3 is used as a constant load of 300 W, while load 4 is emulating a variable load pattern from 500 W to 1700 W with a minimum allowed voltage of 114 V, as shown in Figure 5.33b. Generator 3 is set to inject 300 W during the operation.

After starting and synchronizing generators 1 and 2, the transmission network is configured to feed loads 3 and 4, as described above. A variable load pattern is applied by controlling load 4 while monitoring the load voltage. When the load reaches 1700 W at time 92 s, the load voltage drops to 113 V. Violating the allowed voltage limit triggers a topology reconfiguration from radial to ring by connecting transmission line TL 1-6 at time 104 s. This reconfiguration improves the load voltage profile from 113 V to 115 V, as shown in Figure 5.33c.

The control software for all experiments was completely modeled using Matlab/Simulink. The developed interface toolbox established the communication between the Matlab model and the real hardware components by utilizing the DDS middleware. The entire model is converted to C code and run in real-time. During the operation, the model received measured data at a message rate of 100 Msg/s. The

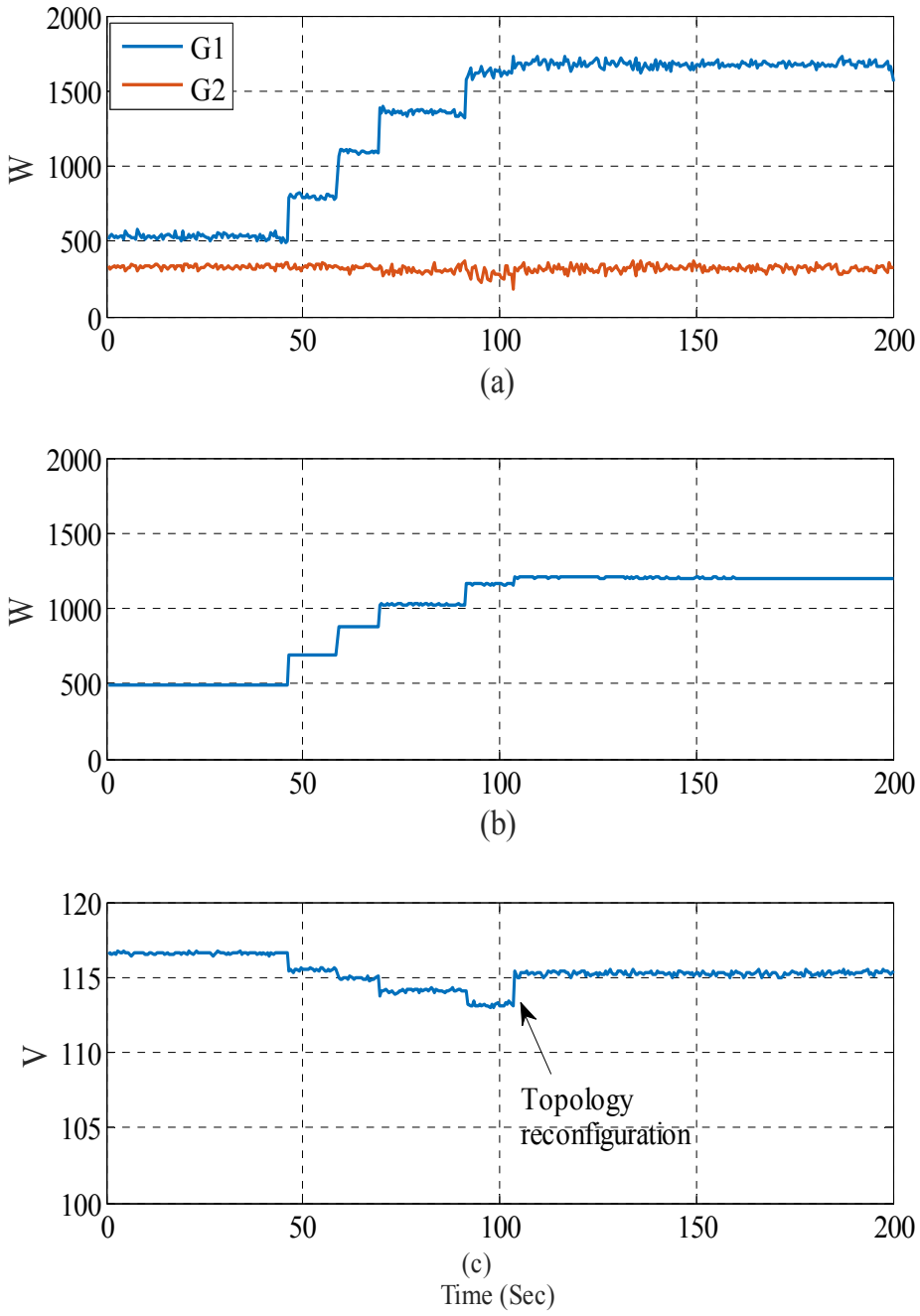


Figure 5.33: Case 3, topology reconfiguration. (a) Output power of generators 1 and 2; (b) load 4 power; and (c) load 4 voltage

experimental results proved the efficiency and reliability of the developed control and communication infrastructure for managing and collecting real-time data from the smart grid testbed. The integration between the modeling and analysis software, and the smart

grid testbed hardware components provides a hybrid hardware-software environment for prototyping and testing developed control and real hardware devices. Fully-automated operation without human intervention was reached using the developed infrastructure. It is worth mentioning that the system is scalable. *i.e.*, it can be expanded to larger systems with a higher number of units and distributed control models run on distributed network resources. Furthermore, the implemented testbed infrastructure allows remote users to connect and perform experiments.

5.6 Summary

In this chapter, the design and implementation of a scalable HIL infrastructure for a smart grid testbed are presented. The developed infrastructure provides the capability of integrating different types of systems and components inside the testbed and connecting several testbeds to study the behavior of complex CPS. The proposed system is based on the DDS standard to provide the low latency communication required for smart grid applications. The used publisher-subscriber scheme provides reliable and flexible communication while eliminating the bottlenecks and a single point of failure. The data structure for the system signals and a Matlab toolbox were developed to allow integration with modeling software, remote monitoring, and control through a computer network. The performance of the developed infrastructure was tested and validated experimentally. The security aspect is addressed by encrypting remote communication using TLS and checks all remote command against physical rules before passing it to testbed devices.

Chapter 6 GPS Based Synchronization Scheme for Distributed DC-DC Converters for Micro Grid application

6.1 Introduction

The new trend in the future in the smart grid network is developing toward Distributed Generations and microgrid. In the microgrid architecture, the energy resources are located close to energy consumers and large units are substituted by smaller ones [65],[66]. The integration of the distributed generation, energy Storage Systems, and consumers' loads through the Point of Common Coupling (PCC) is called a microgrid. A microgrid can be configured into DC and AC microgrid based on the power electronics interface circuits that will be used [67]. Recently, there has been a great interest in utilizing the DC microgrids to integrate distributed resources such as solar panels and energy storage. Since solar panels and energy storage such as batteries and fuel cells generate DC current, DC microgrid provides a flexible and efficient way to integrate these types of resources. Moreover, full converter variable speed wind turbine generation systems usually have an intermediate DC link in the conversion system.

In the DC microgrids, a DC-DC boost converter is a key element to interface distributed generation to the microgrid's DC bus. Various DC-DC boost converters topologies have been studied in [68]-[73]. DC microgrids, along with their DC-DC boost converters, still faces numerous challenges such as ripple contents of the DC bus voltage and current [74]. Indeed, voltage and current ripple are among the various phenomena that contribute to a reduction in lifespan of power sources and energy storage devices interfaced to the DC bus [75],[76].

To overcome this problem, multi-phase interleaved boost converters are used to reduce current and voltage ripple without increasing the switching frequency [77]. The Pulse Width Modulation (PWM) signals of this converter should be generated based on multiple carriers with the same frequency and a different phase shift to reduce the DC-DC converter output voltage ripple. The interleaving technique can be applied to multiphases in a single DC-DC converter or to multiple converters connected in parallel to reduce the voltage ripple and increase efficiency.

The generation and synchronization of the PWM carriers for multiphase converters are quite easy since all the PWM modulators are driven from the same controller and hence the same oscillator**.** However, in distributed resources interfaced with DC-DC converters, each converter has its own controller and hence its own oscillator, which makes the PWM signals synchronization for multiple DC-DC converters a big challenge.

The challenge is related to the frequency drift of each DG's oscillator due to temperature and component tolerance. This drift will create a continuous change in the phase shift angle between PWM carriers of each DC-DC converter [78],[79]**.**

To ensure the most accurate synchronization, it should be taken into account clock drift and oscillator's start latency using hardware-assisted software over software only synchronization. IEEE 1588 time synchronization protocol delivers sub-microsecond synchronization accuracy with hardware assisted [80]. This method can provide very accurate and stable clock signal for all DC-DC converters. However, it assumes that all controllers are connected to a communication network and requires special hardware assisted network switches. Hardware-assisted time synchronization adds extra costs to the

control network, which could be inadequate for small systems. For large distributed system, connecting all controllers to the synchronization network may be infeasible [81]. To solve this problem, a common time reference should be defined and used to adjust the oscillators' frequency. In this chapter, a GPS-based synchronization method is proposed to generate a common time reference to synchronize distributed PWM modulators. Although GPS synchronization has been widely used in the PMUs for synchronized measurements in the AC networks, to the best of the author's knowledge, it has never been used to enhance power quality in DC networks. The proposed method does not need special communication networks between distributed converters for the synchronization process. This synchronization allows the operation of distributed DC-DC converters modulators as interleaved converters system. The interleave operation reduces the ripple and DC-link capacitor size. In addition, it improves the system electromagnetic compatibility by reducing interferences from the ripple.

6.2 DCMG SYSTEM DESCRIPTION

The schematic diagram of DC microgrid and control hierarchy is depicted in Figure 6.1. The microgrid under consideration has three conventional DC-DC boost converters connected in parallel to interface three different energy sources to the common DC bus. One converter will be considered as the master converter and will work in voltage control mode. The main role of this converter is to regulate the DC bus voltage. The other two converters will work in current control mode. Each DC-DC power converter should receive PWM signals from its corresponding local controllers in order to control power flow.

In this work, the local control of each converter should have two types of algorithms. The first algorithm, voltage, and current control algorithm is responsible for controlling the duty cycle of its converter based on the reference power values, which are sent by the energy management system EMS. The EMS should deliver these values taking into account certain criteria, such the energy cost. The detailed operation of the EMS will be discussed in chapter 9.

The second algorithm is the synchronization and carrier generation algorithm. This algorithm will generate a carrier synchronized with the GPS time reference. The phase angle for the generated carrier will be controllable through adjusted offset input.

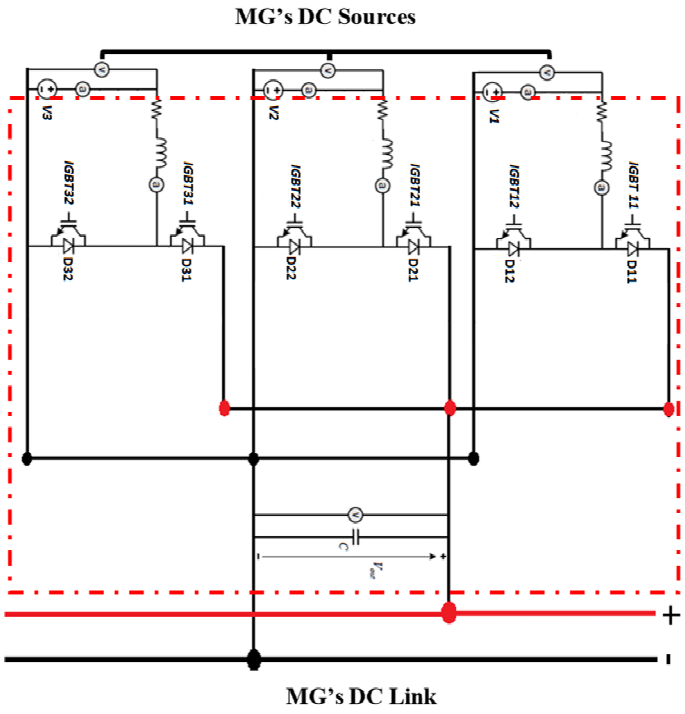


Figure 6.1: Distributed DC-DC converters connected to common DC bus

6.3 DC Microgrid voltage and current control.

Three DC voltage control sources are chosen to emulate the distributed generation in the DC microgrid. These sources are interfaced to the DC bus through a distributed DC-DC boost converter as shown in Figure 6.1. The DC-DC converters parameters are mentioned in Table 6-1. It is assumed that all converters will be controlled simultaneously.

Table 6-1: DC-DC boost converters parameters

Parameters	Value
Inductance	750µ
Inductor resistance	20
Capacitance (C)	312
Capacitor	0.575
DC Bus voltage	50V
DC source 1	25V
DC source 2	22V
DC source 3	20V
Load resistance	4Ω
Switching	2 kHz

The local control of each converter is implemented to control the converter's duty ratio and its PWM carriers. To control the duty cycle of the master DC-DC converter, the voltage and current controllers based on an advanced lead-lag controller (ALLC) are employed during transient and steady-state conditions as shown in shown in Figure 6.2.

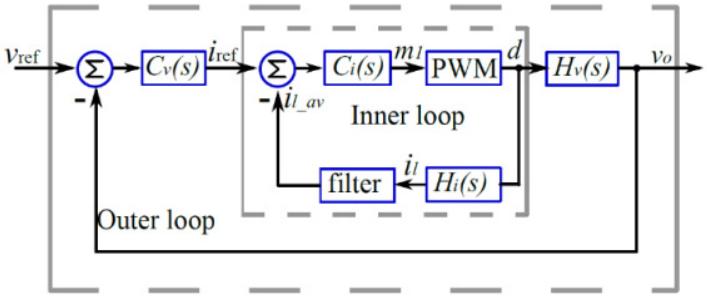


Figure 6.2: ALLC voltage and current control scheme

The current controller based on ALLC is employed for the current controlled converters as shown in Figure 6.3[82][83].

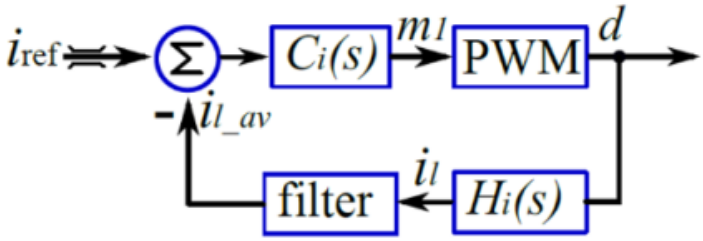


Figure 6.3: ALLC current control scheme

The ALLC controllers are designed based on the Small Signal Model (SSM) using frequency response techniques where $C_v(s)$ is the voltage compensator and $C_i(s)$ is the current compensator that assures cancellation of the static error and high bandwidth. d is the duty cycle ratio that will be compared with PWM carriers to generate the required PWM signal. $H_i(s), H_v(s)$ are the current and voltage transfer functions of the conventional DC/DC boost converters, which shown in equations (6.1) and (6.2).

$$H_v(s) = \frac{V_o\,[n\,R_o(1-mD)^2 - m\,R_l]}{(1-D)\,[n\,R_o(1-mD)^2 + \sigma\,R_l]} \frac{\left(1+{}^{s}/_{\omega_{zv1}}\right)\left(1-{}^{s}/_{\omega_{zv2}}\right)}{\left(\frac{s^2}{{\omega_0}^2}+\frac{2\xi s}{\omega_0}+1\right)} \tag{6.1}$$

$$H_i(s) = \frac{V_o\,(m+\sigma)}{\sigma\,R_l + n\,R_o(1-mD)^2} \quad \frac{\left(1+{}^{s}/_{\omega_{zi}}\right)}{\left(\frac{s^2}{{\omega_0}^2}+\frac{2\xi s}{\omega_0}+1\right)} \tag{6.2}$$

The double pole frequency ω_0 depends on the input voltage (V_{in}) and the nominal output voltage (V_o) as well as inductance (L) and output capacitance (C). It is also important to note that ω_0 depends on the load resistance (R_o), the internal resistance of the inductor (R_l) and the internal resistance of the capacitor (R_c), which shown in equation (6.3)

$$\omega_{zi} = \frac{1}{C\left(R_c + \frac{\sigma R_o}{m+\sigma}\right)} \quad \omega_{zv1} = \frac{1}{C\ R_c} \quad \omega_{zv2} = \frac{n\,R_o(1-mD)^2 - m\,R_l}{m\,L} \tag{6.3}$$

The system damped ratio ξ for both transfer functions is given by equation (6.4).

$$\xi = \frac{\sigma\,L + C\,[\sigma\,R_l\,(R_o+R_c) + n\,R_c\,R_o(1-mD)^2]}{2\,\sqrt{\sigma\,L\,C\ (R_o+R_c)[\sigma\,R_l + n\,R_o(1-mD)^2]}} \tag{6.4}$$

Where D is the nominal duty ratio, n is the number of phases, and m is the number of parallel switches per each phase which their values are equal to one for the conventional boost converters shown in Figure 6.2.

6.4 Synchronization and carrier generation algorithm

The GPS is a navigation system that consists of 24 satellite positioned in six orbital planes [84]. Each satellite has an onboard atomic clock that provides a precise time reference. The GPS satellites broadcast a microwave signal that received by the GPS receiver on the earth surface. The GPS receiver processes the signal from three or more satellites and computes the position and current time with high accuracy. The receiver output the calculated time in the form of a serial stream or one pulse per second (1PPS). The one pulse per second output is derived from the satellite atomic clock and has the accuracy to few tens of nanoseconds. A synchronized signal with higher frequency for carrier generation can be generated from the 1 Hz GPS clock reference using frequency multiplier. The standard frequency multiplier consists of phase locked loop PLL and a frequency divider in the loop as shown in Figure 6.4.

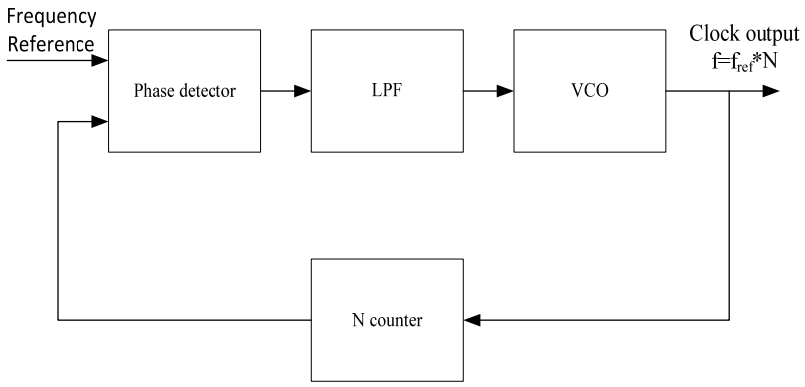


Figure 6.4: Frequency multiplier using PLL

The 1 Hz frequency reference is compared with the voltage controlled oscillator (VCO) frequency output after dividing by the N counter using phase detector. The phase detector output is filtered and then used to control the VCO output frequency. The phase detector filtered output will accelerate or decelerate the VCO based on the phase between the reference signal and the counter output. When the counter output has the same frequency and looked with the reference signal, the phase detector output will hold the voltage that produces this frequency. The phase angle between the output signal and the reference signal can range from 0 to 90 degree based on the phase detector type. Generating high-frequency clock from very low-frequency reference (1 Hz in the case of GPS reference) requires high division factor in the loop. For example, generating 100,000 KHz requires 1/100,000 divider in the loop. The high dividing factor introduces a long delay, which makes it difficult to stabilize the PLL frequency output.

A digital PLL (DPLL) is used to multiply the 1 Hz frequency reference and overcome the stabilization problem. The proposed DPLL is shown in Figure 6.5.

A positive-edge-triggered phase comparator is used to compare the 1PPS signal with the signal generated from the VCO divided by the digital counter. The phase comparator

output pulse width represents the phase between the GPS reference signal and the VCO output frequency. The pulse width is converted to a stream of high-frequency pulses by gating a high-speed oscillator output with AND gate. This pulses stream is converted to digital counts by a digital counter. An edge detector generates a pulse that latches the digital count in a data latches each cycle. The latch output is converted to analog voltage and connected to the VCO frequency control input. The analog voltage level will change depending on the phase angle between VCO and GPS reference signal. The VCO is designed to generate the required output frequency at voltage level equivalent to 180-degree phase angle. Since the counter output is inverted, the signal output will be in phase with the GPS reference. A fail-safe logic constantly monitors the counter output to determine the lock status of the PLL. If the PLL fails to lock with due to the absence of the reference signal, the fail-safe logic switches the VCO control to a stable frequency reference.

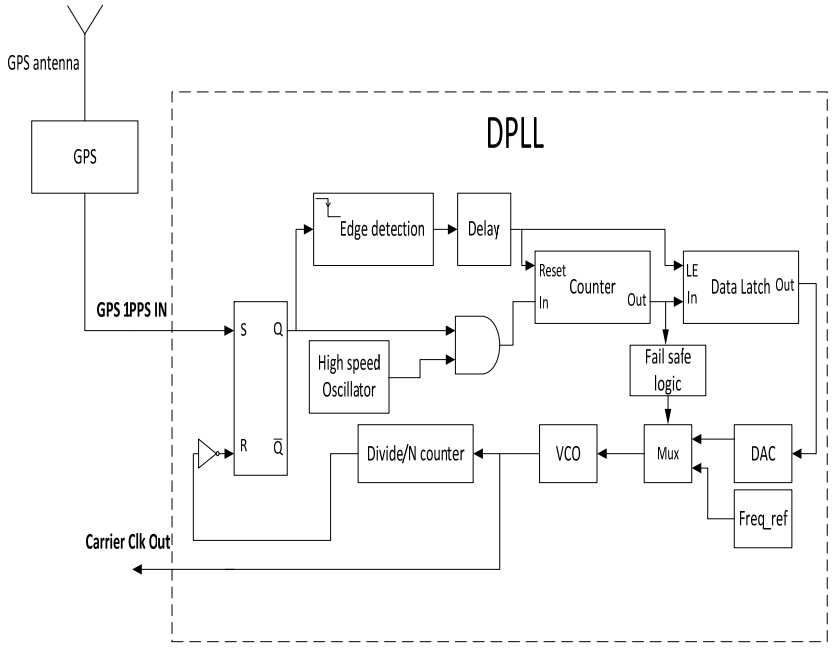


Figure 6.5: Digital phase locked loop DPLL

To test the performance of the proposed frequency multiplier based on the DPLL, a simulation model is built using Matlab/SIMULINK simulation software. The block diagram for the simulation model is shown in Figure 6.6.

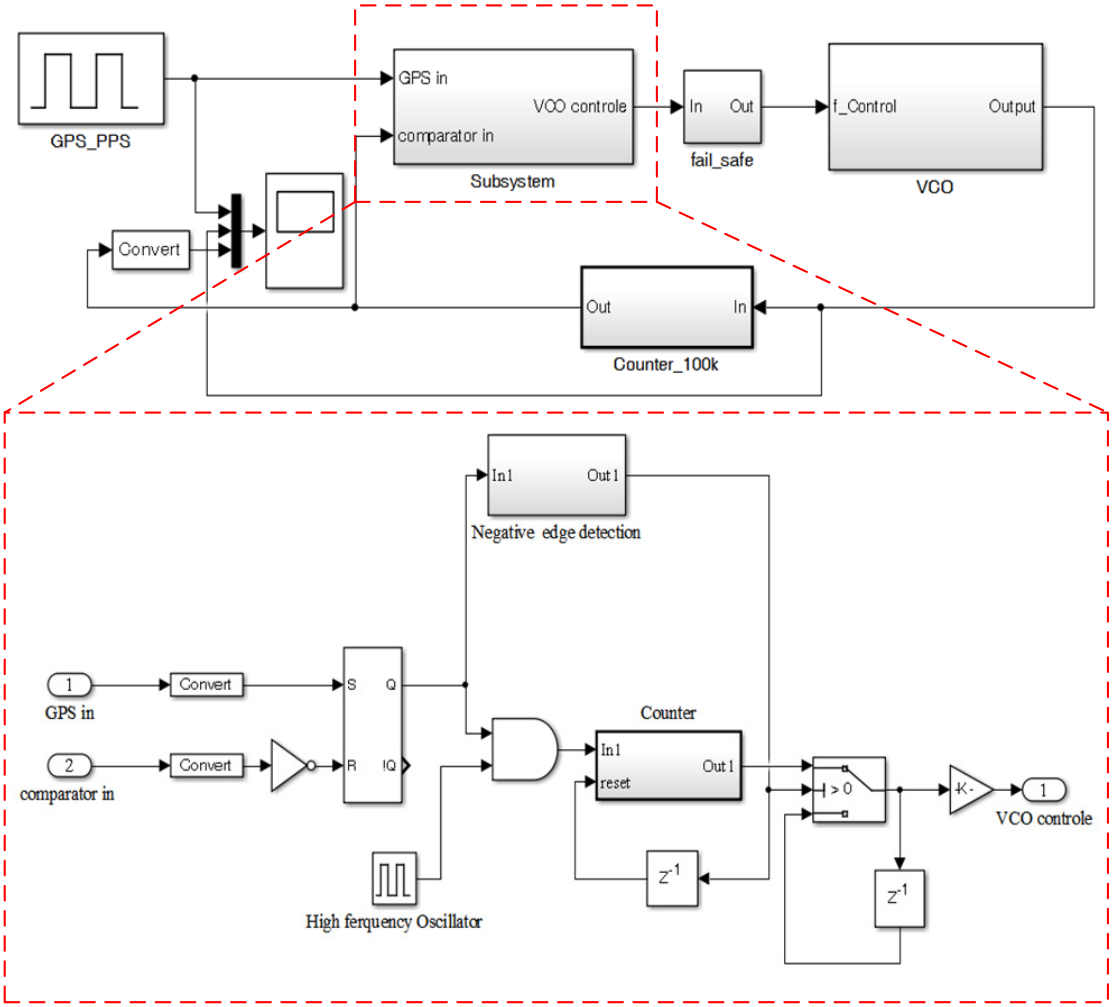


Figure 6.6: DPLL SIMULINK Simulation Block Diagram

The performance of the proposed DPLL is depicted in Figure 6.7. At the beginning of the simulation, the frequency divider output frequency was lower than GPS reference and has a large phase difference, as shown in Figure 6.7-b. Due to the existence of the large phase shift, the VCO voltage increases and leads to the higher output frequency, as

shown in Figure 6.7-c. As a result of increasing the VCO frequency, the phase shift starts to decrease between generated signal and the GPS reference signal. After 5 cycles, the generated signal is locked with the GPS reference signal and has the same frequency and phase angle, as shown in Figure 6.7- a and Figure 6.7-b. Figure 6.7-c shows the 100Khz frequency generated by the VCO. This high-frequency output will be used as a synchronized clock for the carrier generation module.

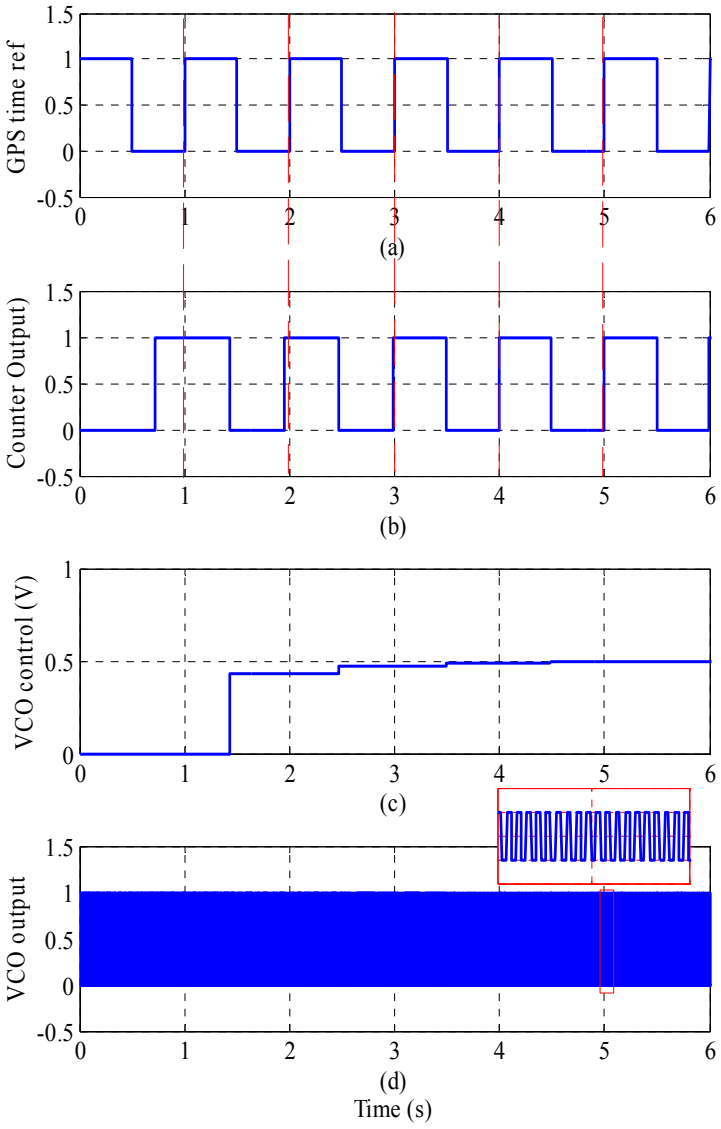


Figure 6.7: Propose DPLL simulation performance

6.5 PWM carrier generation

In this stage, a synchronized saw-tooth carrier will be generated. The carrier generation module will receive three inputs, carrier clock, 1PPS from the GPS and adjustable offset. A digital counter will be incremented at the positive edge of the carrier clock. When the counter reaches the peak value, reset logic will reset the counter to zero to generate the saw-tooth signal. To ensure the saw-tooth signal is synchronized with the edge of the 1PPS GPS reference, the counter's initial value will be set at the positive edge of the 1PPS signal. The generated saw-tooth signal phase is adjusted through the offset input. Each time the user adjusts the phase angle the difference between current offset and previous offset is calculated and added to the counter. To maintain a fixed phase angle the offset value is loaded as an initial value at the positive edge of the 1PPS signal. A simulation model is built using Matlab/SIMULINK to test the carrier generation module.

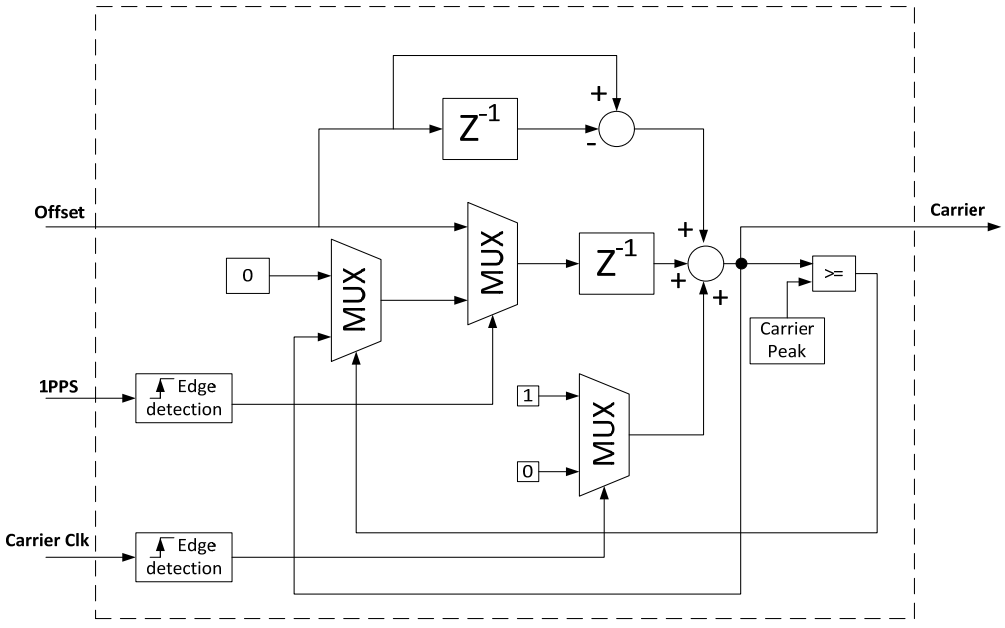


Figure 6.8: Synchronized PWM carrier generation

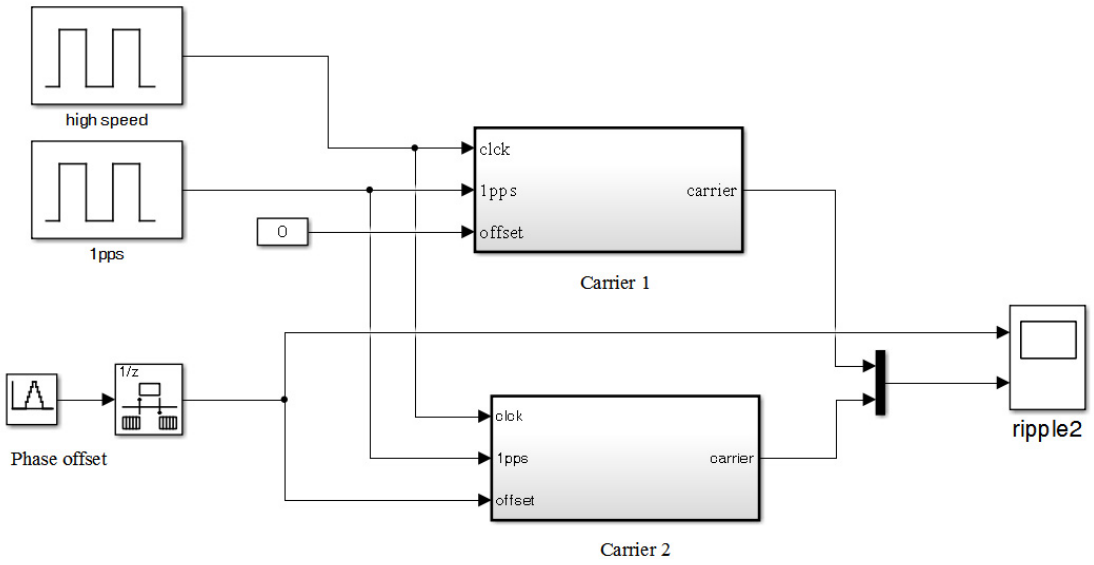


Figure 6.9: Phase adjustment simulation model

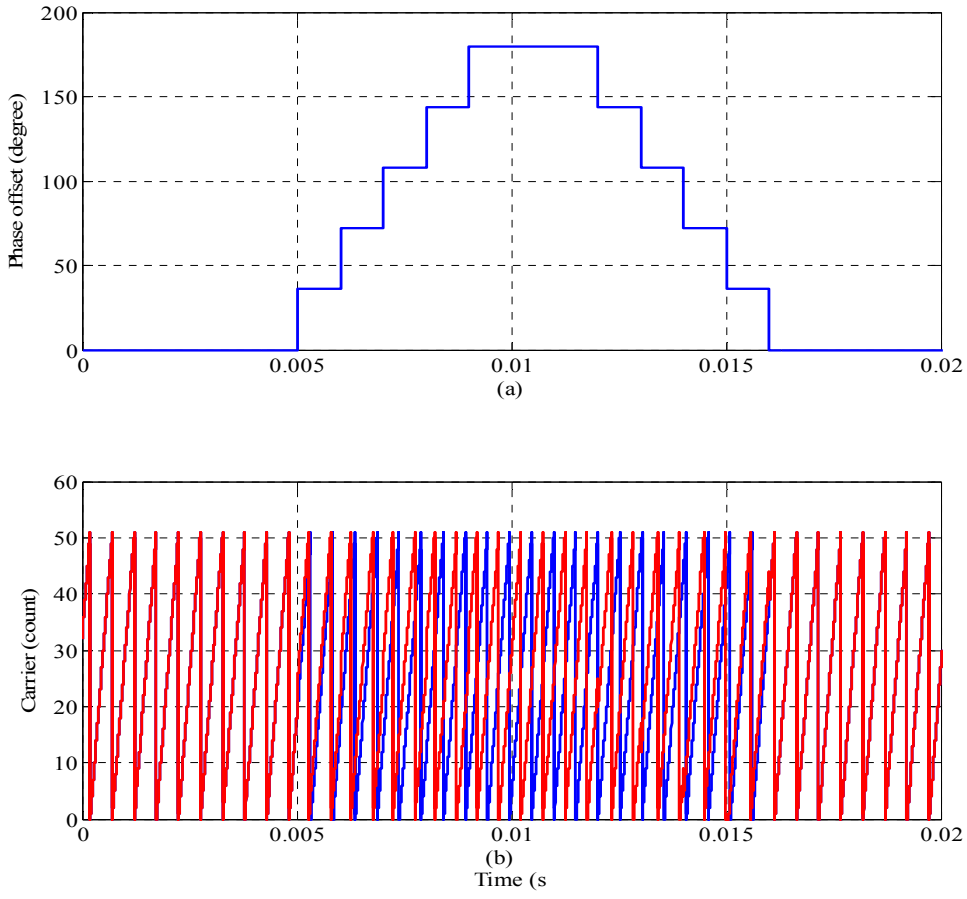


Figure 6.10: carrier phase adjustment performance

The simulation model for the carrier generation is shown in Figure 6.9. Two carrier modules were simulated. The phase offset for the first module is set to zero to maintain zero phase angles with respect to the GPS signal. The second carrier's phase angle is incremented from zero to 180 degree. The simulation results are shown in Figure 6.10. The phase offset for carrier module 2 is shown in Figure 6.10-a. Figure 6.10-b shows the phase angle for both carrier modules. The simulation starts with zero phase angle between the two carriers. At time equal to 0.005 sec, the phase offset increment gradually from zero to 180 degree. As depicted from Figure 6.10-b, the second carrier phase angle follows the phase offset input and shifted with respect to carrier 1. When the phase offset is set back to zero, the two carriers are locked in phase. The phase offset between carriers can be controlled manually or through automatic search algorithm to optimize the DC bus voltage ripple. The automatic adjustment of the phase offset will be discussed in detail in the next chapter.

6.6 Simulation results

A simulation model for three parallel converters connected to a common DC bus built based on MATLAB/SIMULINK® to test and validate the robustness of the proposed GPS-based synchronization methods. The converters connection topology and parameters are shown in Figure 6.1 and Table 6-1. One of the converters controllers is designed to operate in voltage control mode, while two controllers are designed as a current controller as discussed earlier. The load current is shared equally between the three converters. To evaluate the performance of the synchronization algorithm and its impact on the DC bus voltage ripple, first, the simulation is started with zero phase offset between the three

converters carriers. After a short period, the second converter's carrier phase is adjusted to 120 degrees with respect to the reference signal. Then, the third converter carrier phase is adjusted to 240 degree. The simulation results are shown in Figure 6.11. At time equal to 1 sec, the angle for the second converter carrier is set to 120 degrees, as result of changing the phase angle, the DC bus ripple is reduced from 1.72 V RMS to 1.063 V RMS. At time equal to 2 sec, the angle for the third converter carrier is set to 240 degrees, the voltage ripple is reduced significantly from 1.063V to 0.15 V RMS.

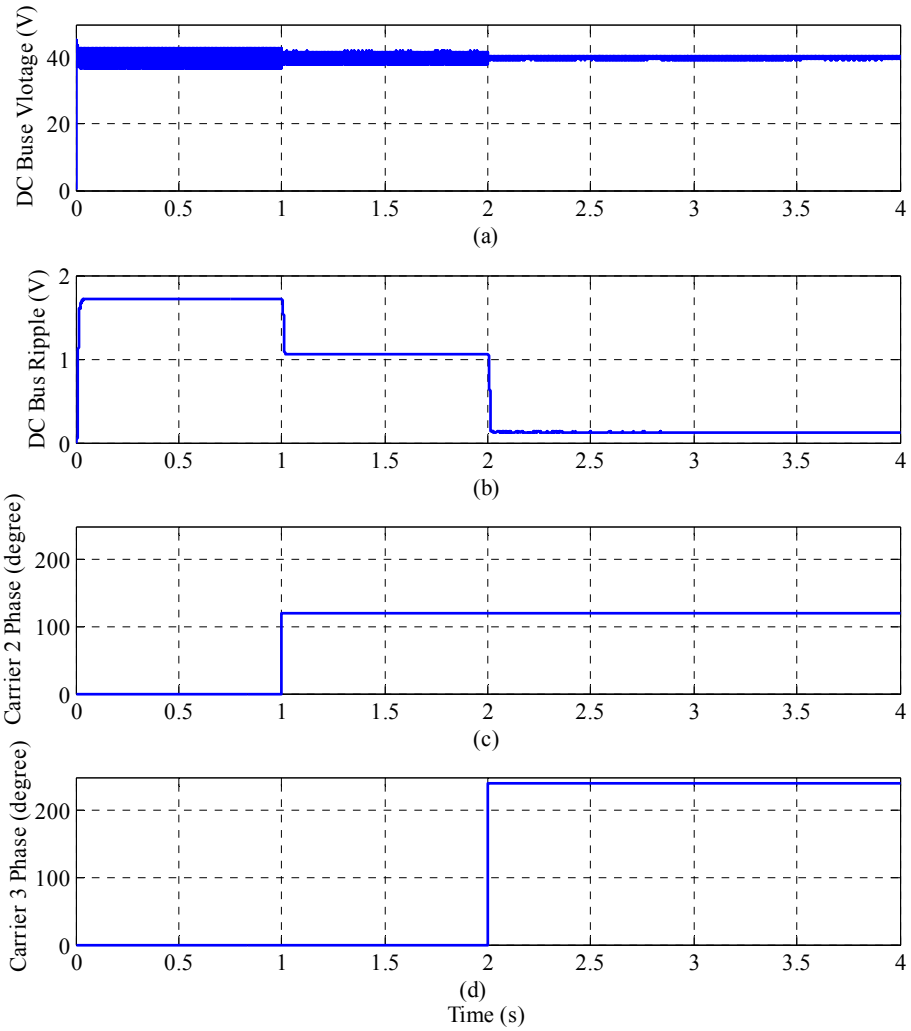


Figure 6.11: Multiple converters synchronization performances (a) DC bus voltage, (b) ripple RMS, (d) carrier 1 phase angle, (e) carrier 2 phase angle

6.7 Hardware verification and experimental result

In order to implement the GPS synchronized carrier generation for distributed DC-DC converters in real-time, an experimental test bench has been designed. In this implementation, a GPS time reference module based on Venus838LPx_T GPS receiver shown in Figure 6.12 is used.

Error! Reference source not found. GPS timing Module

The Venus838LPx_T is a single chip GPS receiver that can generate 1 PPS reference time signal with 6 ns accuracy. The GPS can generate a time reference with one satellite in view. Moreover, the module has a built-in programmable PLL that produces variable frequency output ranging from 1 to 10 MHz, in this setup, the PLL is programmed to produce 100 KHz clock frequency. The output frequency is controlled using the control panel shown in **Error! Reference source not found.**. The phase angle between the 1PPS time reference and programmed PLL output is shown in Figure 6.14. As depicted from the, figure the module produces a high-frequency clock locked with the GPS 1PPS.

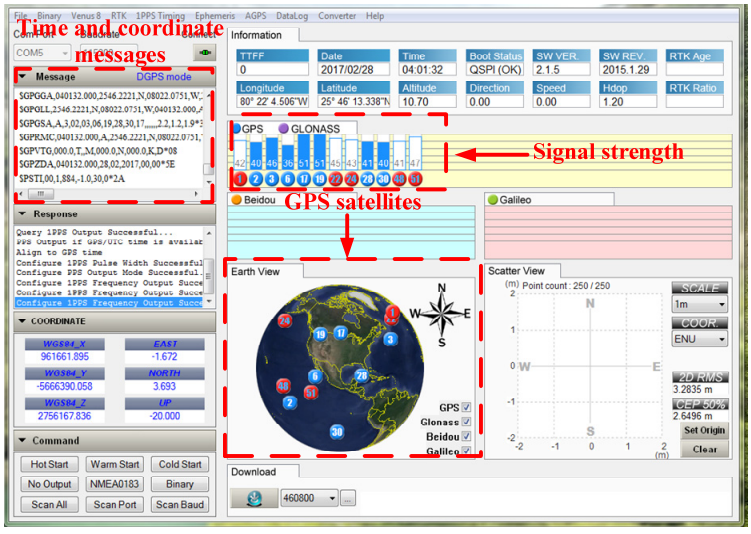


Figure 6.12: the GPS software control panel

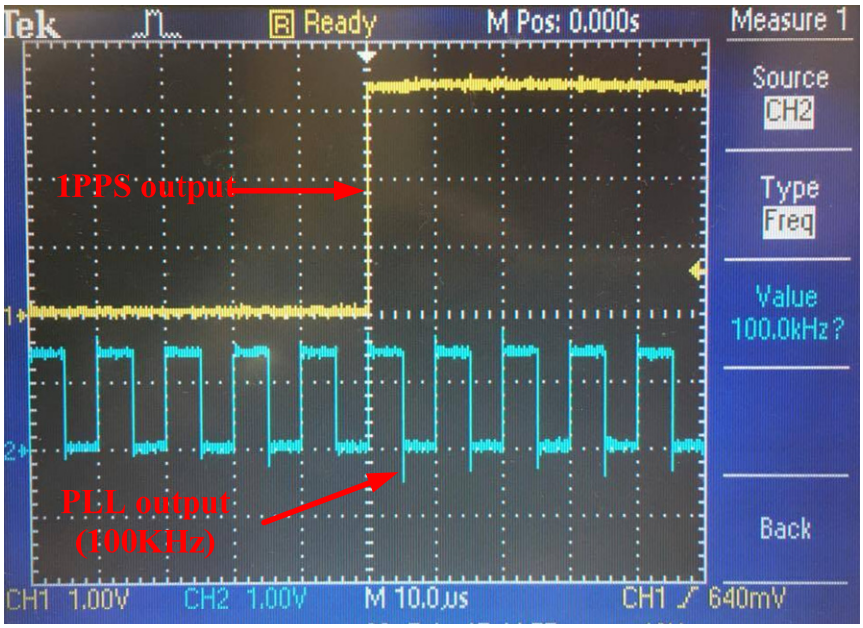


Figure 6.13: 1PPS and high-frequency output signal

The PLL output and the 1PPS are connected to an ARM Cortex M4 Microcontroller. The ARM microcontroller is used to implement the functions of the carrier generation and PWM. This control layer performs fast computation for the proposed algorithms and hard-real-time input/output function to control the DC-DC converters semiconductor switches. The high-speed PLL output is connected to the microcontroller interrupt input. The interrupt subroutine is executed 100K times/ s. Each interrupt call, the subroutine reads the offset angle, samples the 1PPS input and increments the counter to generate the saw-tooth carrier. Each saw-tooth cycle, the Microcontroller compares the carrier with the reference received from the dSpace 1004 to generate the PWM output. The STM32f407vgt6 32 Bit ARM cortex M4 processor running at 160MHz was used for the embedded implementation of the proposed algorithm.

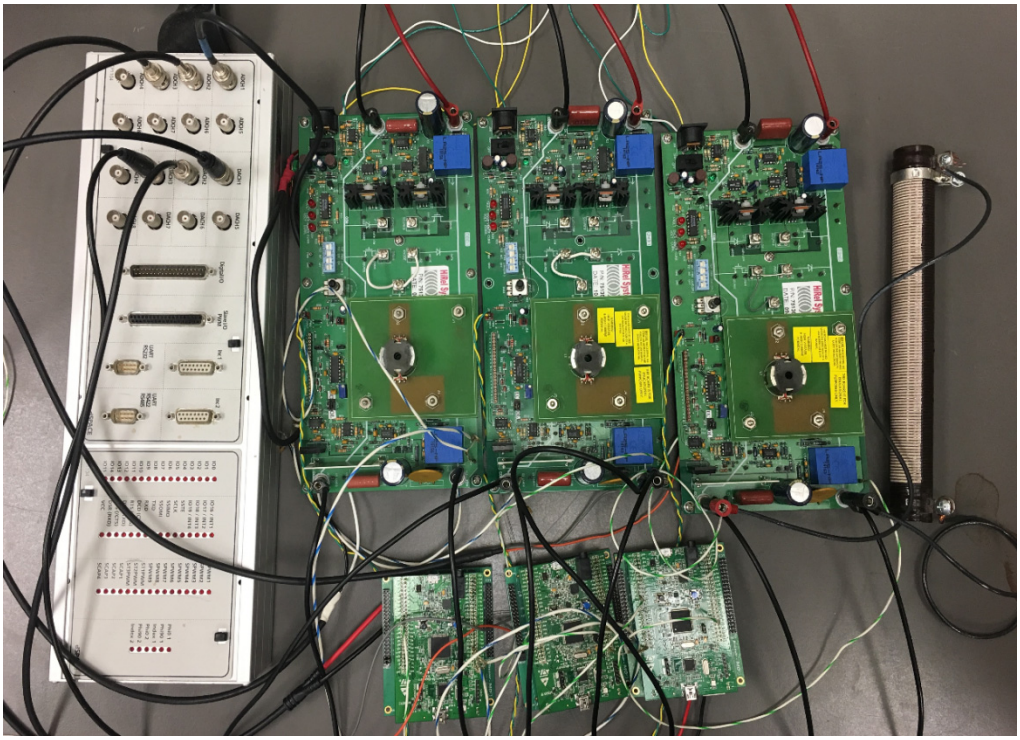


Figure 6.14: Hardware setup for the GPS carrier synchronization

The embedded firmware is generated from Simulink model and compiled using GNU C cross-compiler for ARM. The voltage and current control loops are implemented in a dSpace 1104 embedded controller. The duty cycle reference is transferred from the dSpace to the ARM processor as an analog reference.

The power circuit consists of three converters connected to 4 Ohm load and 40 V common DC bus. The controllers for the three converters are adjusted to equally share the load current.

Figure 6.15 shows the DC bus voltage ripple before and after carrier phase angle adjustment, respectively. At time equal to zero, all carriers were synchronized with zero phase angle and the ripple was at the maximum value. At time equal 3. 5 s, the second converter carrier phase is adjusted to 120 phase angle with respect to the first converter.

At time equal to 4.8 s, the third converter carrier phase is adjusted to 240 degrees. As depicted from Figure 6.15, the phase adjustment reduces the ripple magnitude from 4 V to 1.6 V with adjusted carrier phase angle.

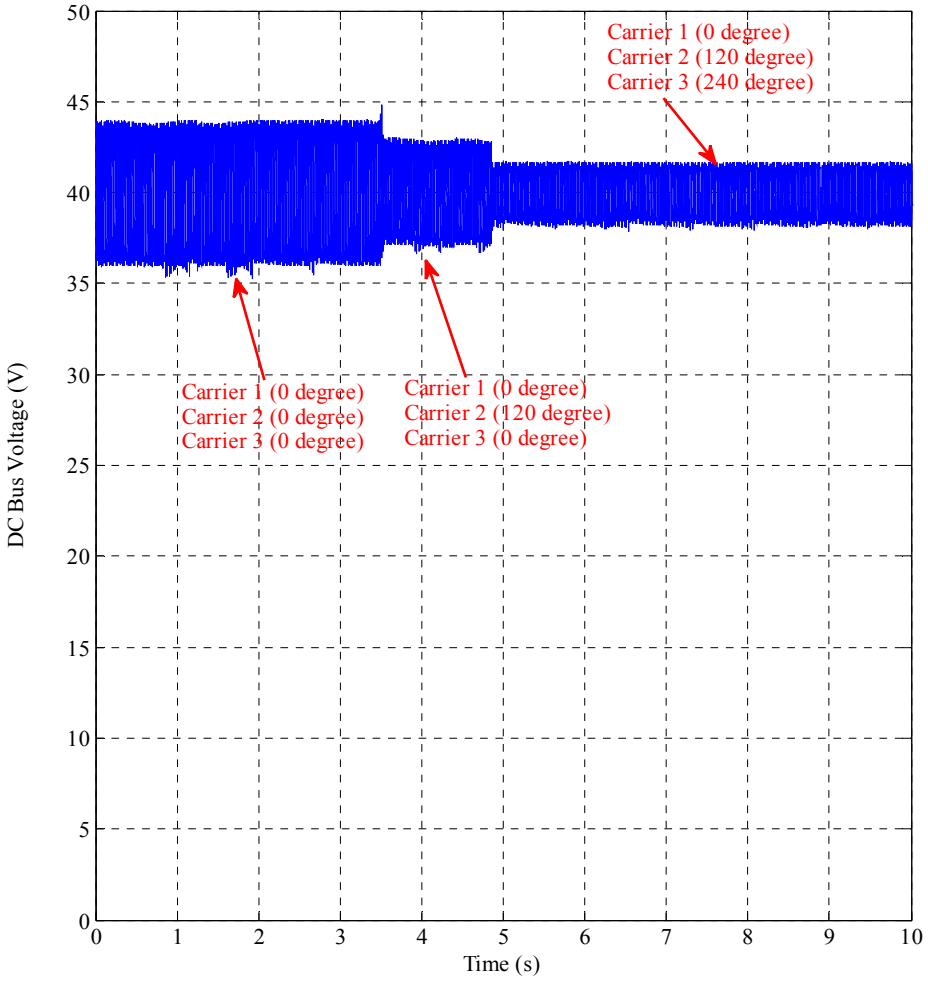


Figure 6.15: DC bus voltage with adjustable carrier phase angles

6.8 Summary

In this chapter, a synchronization method based on the GPS common time reference for PWM carriers of DC-DC is proposed. The GPS synchronization is well known in the AC network; however, the proposed technique extends the application of GPS synchronization to DC microgrid. The proposed method does not need special

communication networks between distributed converters or hardware assisted network switches such as IEEE 1548 precision time Protocol. The proposed synchronization and carrier generation algorithm allows the operation of distributed DC-DC converters modulators as one interleaved converter. The interleaved operation of the multiple converters improves the power quality without increasing the size of passive element filters or the switching frequency. The simulation results and experimental verification show the success of the proposed synchronization method in minimizing the DC bus voltage ripple.

Chapter 7 Carrier Extraction Based Synchronization Scheme for Distributed DC-DC converters

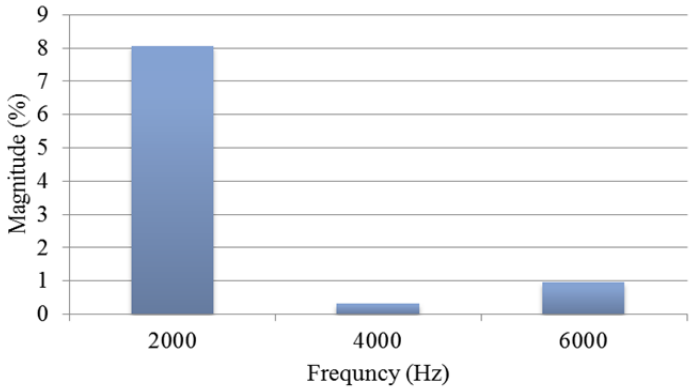
7.1 Introduction

GPS provide an excellent time reference for synchronization and phasor measurement, however, GPS signal is prone to jamming, spoofing and blocking. Sensitive systems should have a backup or alternative synchronization method to prevent degradation of system performance. In this chapter, a new method for synchronizing PWM modulators of distributed DC-DC converters is presented. The proposed synchronization method utilizes the ripple on the DC bus as a common frequency reference. In this scheme, one converter will be chosen to regulate the carrier frequency of the DC bus. The other converters in the system will extract the carrier frequency components from the DC ripple and synchronize their local oscillators with the master carrier. To adjust the carrier phase angle for each converter to an optimum value, a new Phase Shift Control Algorithm (PSCA) is developed. The PSCA is inspired from carrier sense multiple access communication (CSMA) media access control protocol. The PSCA is completely distributed and doesn't require a communication channel between converters

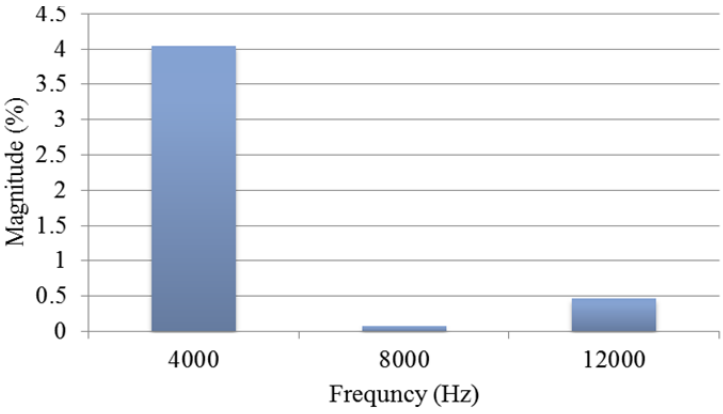
7.2 Carrier frequency and angle extraction

Power electronics converters use pulse width modulation PWM to control output voltage or current. The modulated output voltage is composed of the average DC value and voltage ripple. The AC voltage ripple consists of dominant frequency components equal to the carrier frequency used by the PWM modulator and multiple harmonics.

Figure 7.1 shows the harmonics contents of the DC-DC boost converter output voltage at different carrier frequencies. As depicted from the figure, the dominant frequency content is always equal to the carrier frequency, with 8% and 4% relative to DC magnitude at switching frequency equal 2 KHz and 4 KHz, respectively. If one converter is selected to operate as a DC bus master and regulate the carrier frequency, this frequency component can be extracted and utilized as a common frequency reference for other converters connected to the same DC bus.



(a)



(b)

Figure 7.1: Harmonics content of DC-DC boost converter output. (a) 2 KHz switching frequency, (b) 4 KHz switching frequency

To extract the carrier frequency from DC bus voltage ripple, each converter controller will run the extraction algorithm shown in Figure 7.2. The algorithm uses a band pass filter (BPF) to isolate the ripple component associated with the carrier frequency from the measured DC voltage. The BPF will be tuned to pass only carrier frequency and reject all other harmonics. This is necessary to reject any harmonics produced by nonlinear loads. The filter output will have the same master converter switching frequency and fixed phase angle with respect to the master carrier. The upper and lower bands of the BPF are defined based on the allowed switching frequency range. The output of the BPF will be considered as the DC bus's carrier frequency reference (Bus_{cr}).

For algorithm verifications, the DC bus voltage for boost converter with 2 KHz switching frequency shown in Figure 7.3 (a) is fed into the BPF. The BPF isolated the AC carrier component of the signal, as shown in Figure 7.3 (b). Next, the AC carrier was fed into a PLL algorithm which, in its turn, accurately estimated the AC carrier's frequency, shown in Figure 7.3 (c), and phase angle, shown in Figure 7.3 (d). Then, a peak detector estimates the magnitude of the DC voltage ripple, which is shown in Figure 7.3 €. Finally, we notice a fixed phase angle difference between the AC carrier and the master carrier shown in Figure 7.3 (f). This is because of the delay imposed by the filter. This phase shift will not impact the final synchronization or optimization process since it is fixed and the search algorithm will adjust the final phase angle.

For fail-safe operation, the PLL internal oscillator is designed to operate in the allowed switching frequency band only; if slave converters lost the synchronization signal, the PLL oscillator will continue to produce switching frequency within the

allowed band. Since the carrier frequency has the highest magnitude of the DC bus voltage ripple, a peak detector is used to detect the magnitude of the BPF output each switching cycle. The output of the peak detector is averaged to suppress measurement noise and used as an indicator for the DC bus's ripple magnitudeBus_{crmag}.

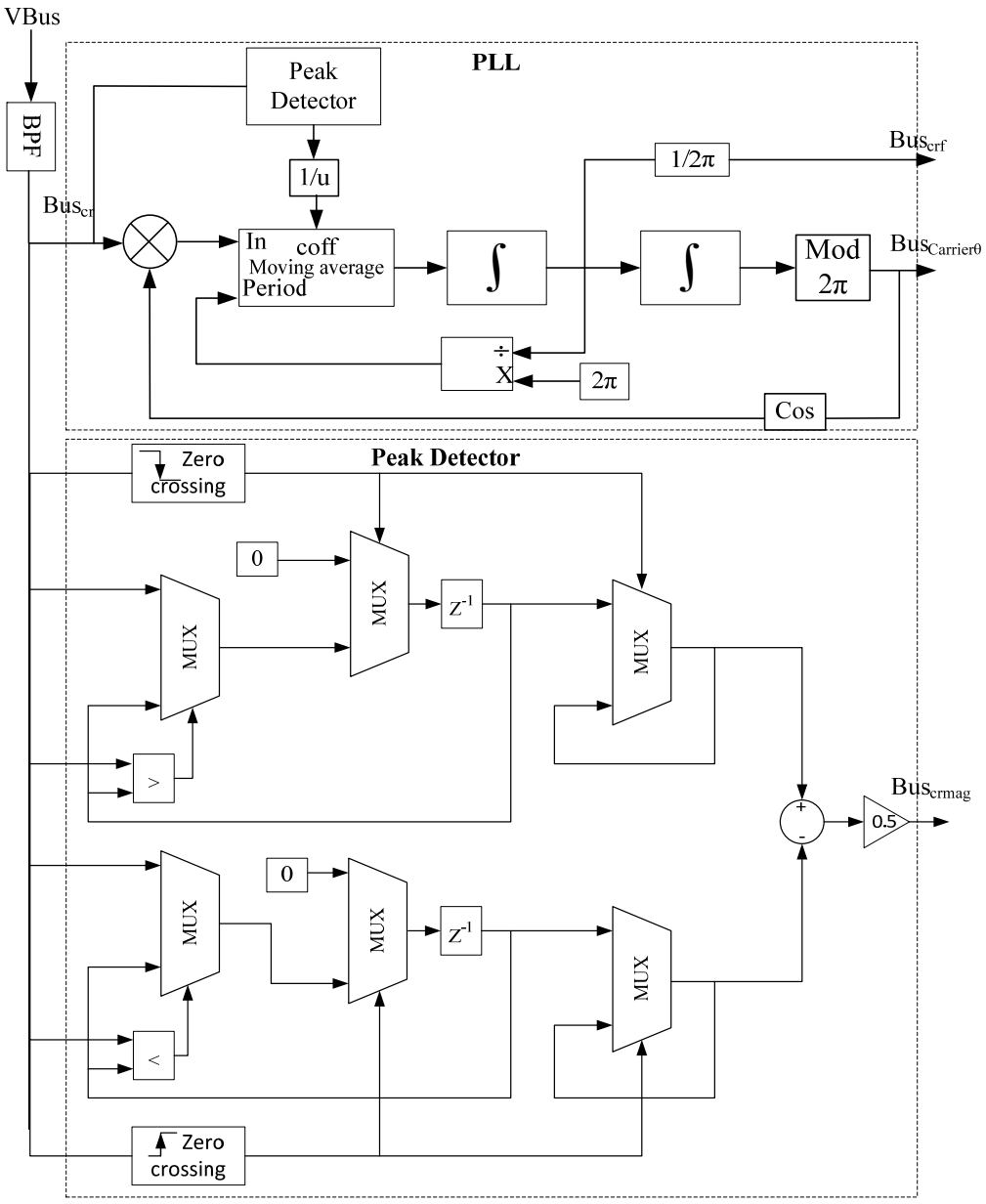


Figure 7.2: DC bus carrier frequency and magnitude extraction algorithm block diagram

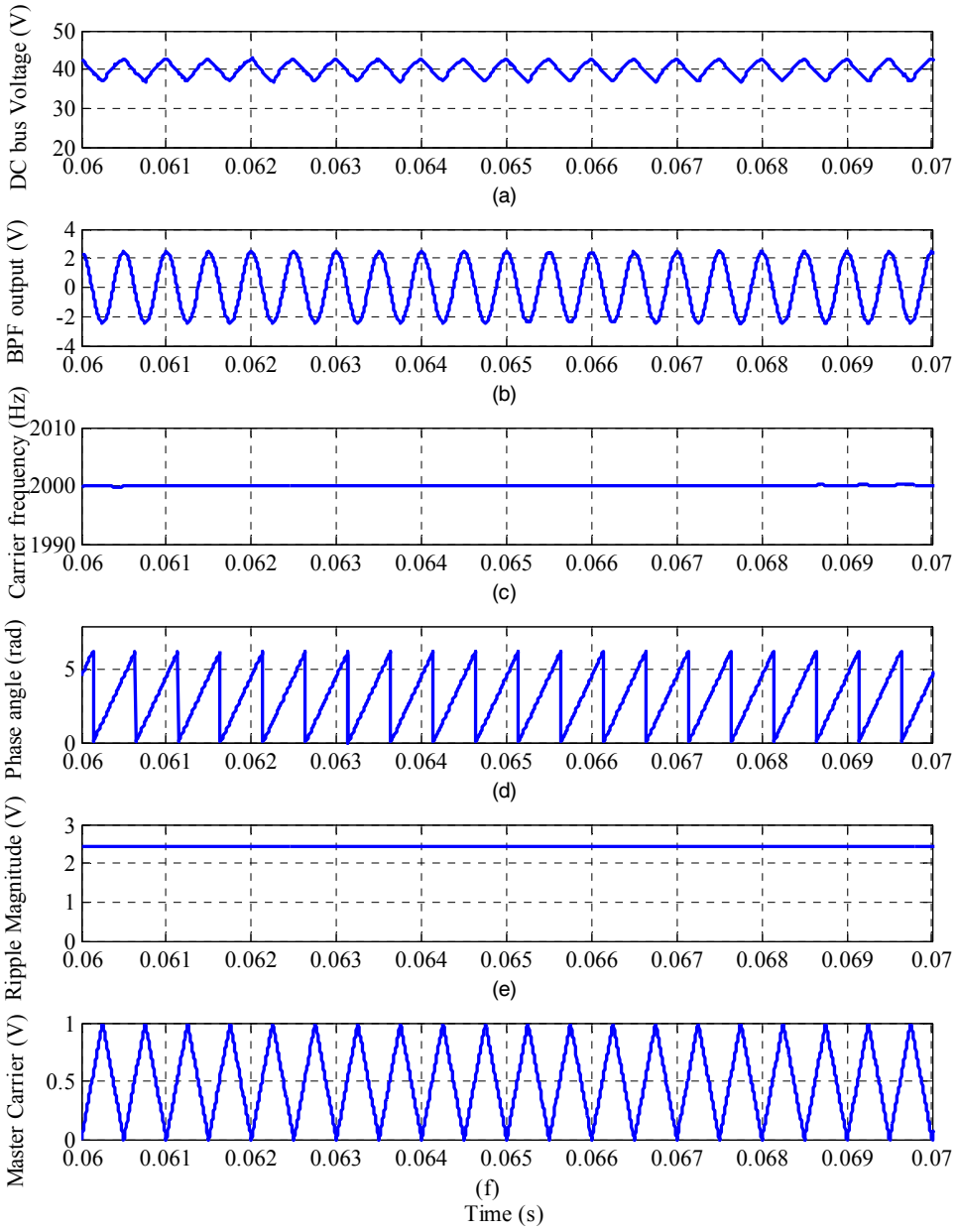


Figure 7.3: Phase locked loop and peak detector output. (a) DC bus voltage, (b) bandpass filter output, (c) estimated frequency, (d) carrier phase angle, (e) master carrier

7.3 PWM carrier generation

In this step, each converter controller will run a local software oscillator. The software oscillator will receive Bus_{crf} and $Bus\_Carrier_{\theta}$ from local PLL to generate its local carrier ($Convx_{cr}$) as shown in Figure 7.4. The carrier generator integrates the

estimated frequency and generates a saw tooth with 2π peak value. The phase angle of the saw tooth signal is adjusted to match the angle of the master carrier. This step is essential in order to keep $Convx_{cr}$ synchronized to the DC bus's carrier frequency. Then the saw tooth signal is converted to a carrier signal with a triangle shape. The phase angle of each local oscillator carrier $Local\_Carrier_{\theta}$ will have the same angel as the $Bus\_Carrier_{\theta}$. An offset angle θ_x can be added to control the desired phase shift. The phase angle offset will be controlled by the search algorithm. As a result, all slave converters PWM carriers will have a frequency value equal to Bus_{crf} and the phase angle equal to $Bus\_Carrier_{\theta}$.

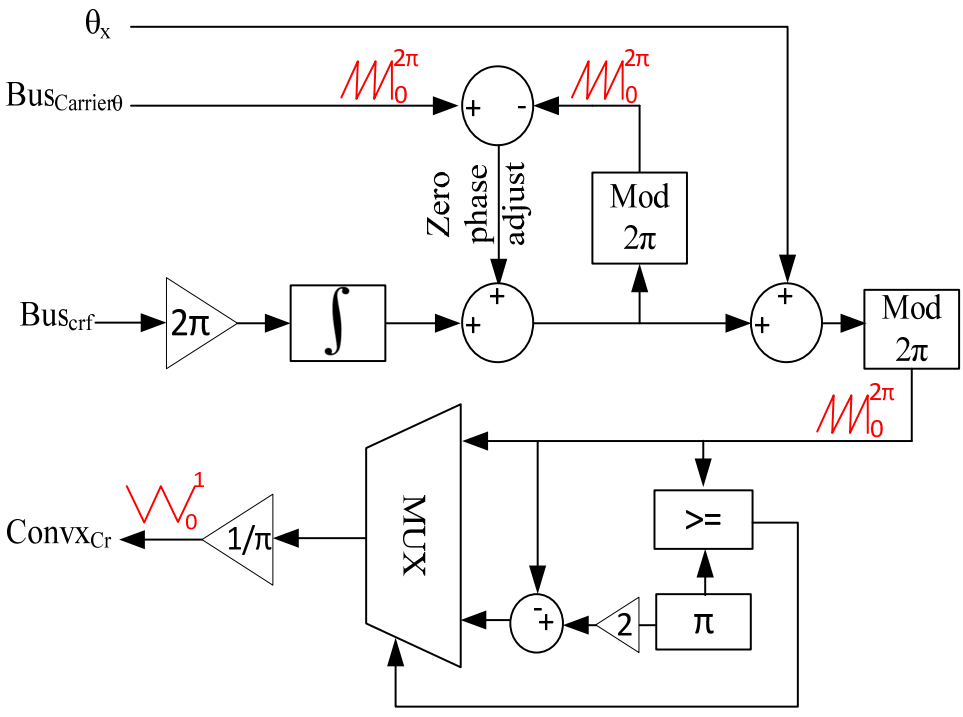


Figure 7.4: PWM carrier generation block diagram

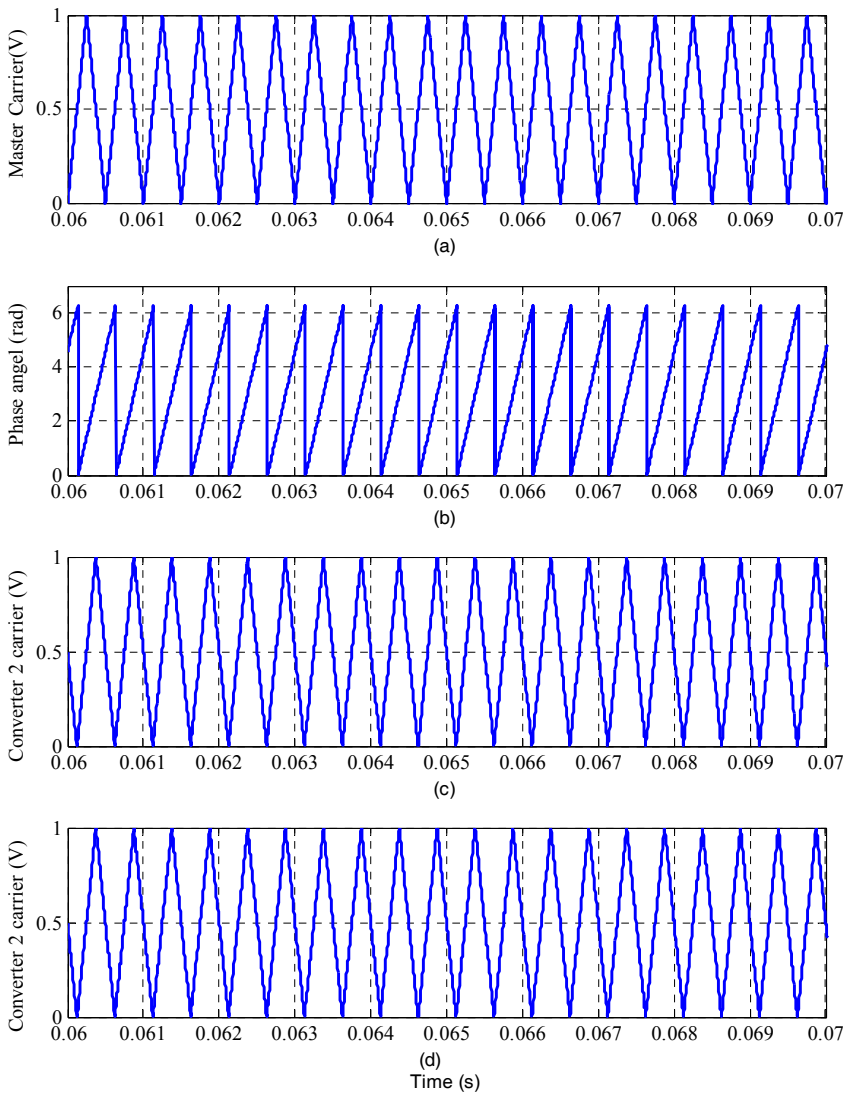


Figure 7.5: synchronized carrier generation. (a) Master carrier, (b) master carrier phase angle, (c) converter's 2 carrier, (d) converter's 3 carrier

Figure 7.5 shows the generated synchronized carriers. Master carrier and extracted phase angle are shown in Figure 7.5 (a) and (b) generated synchronized carriers for two different converters are shown in Figure 7.5(c) and (d). As depicted in Figure 7.5, the proposed algorithm succeeds to generate synchronized carrier with fixed phase angle with respect to the master carrier. The fixed phase shift can be compensated by adding phase offset to cancel the filter delay.

7.4 Phase angle control algorithm

Each converter will have a local controller that consists of carrier extraction and synchronization module, PSCA module, pulse width modulator, voltage and current controller, as shown in

Figure 7.6. Following the synchronization process, the PSCA will work to minimize DC bus ripple magnitude by adjusting the phase offset for each converter carrier.

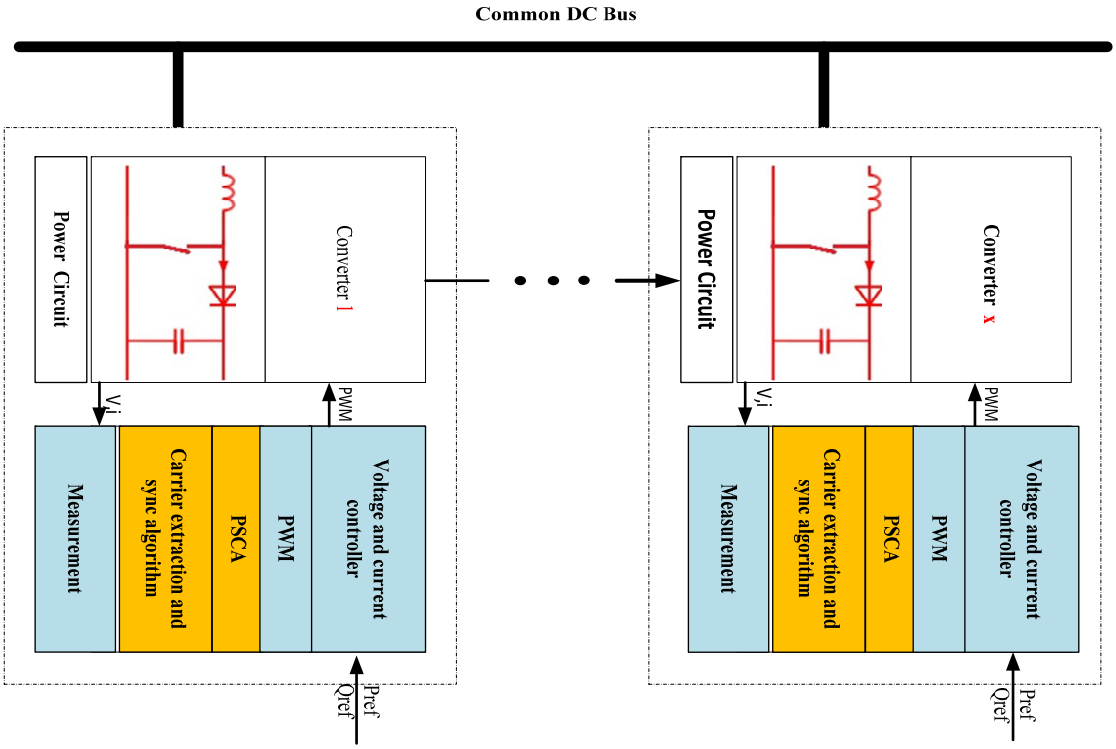


Figure 7.6: Multiple converters with carrier extraction and PSCA block diagram

The PSCA operation is inspired from CSMA MAC protocol. All converters connected to the DC bus will use PSCA to control the local oscillator phase angle except the master converter. The PSCA should increment the phase angle while monitoring the ripple magnitude until reaching the optimal phase angle that produces a minimum ripple.

Since multiple converters will be connected to the same DC bus and search for the optimal angle, it is possible for two or more converter to change their phase angle at the same time. Changing the angle for more than one carrier simultaneously could disturb the PSCA.

To avoid disturbing the PSCA by changing the phase angle of multiple carriers simultaneously, the PSCA utilize the same technique used by CSMA. CSMA detects whether another transmission is in progress by detecting the presence of a carrier. If a carrier is present, the transmitter waits for a random time before trying to initiate transmission again. In the same manner, PSCA monitors the carrier magnitude before initiating phase control algorithm. If a change in the carrier magnitude is detected, the PSCA will set a flag to indicate detection of another converter and wait a random time before trying to modify the phase angle, as shown in Figure 7.7. To avoid the impact of noise and load change on the carrier magnitude, the PSCA will ignore magnitude changes less than a predefined threshold. If there is no activity detected, PSCA will start searching for the optimum angle using the perturb and observe technique. The PSCA will increment the phase angle by a small step and observe the effect on the ripple magnitude if the ripple is reduced the PSCA will continue incrementing the phase angle until the ripple starts to increase again. Perturb and observation algorithm will oscillate around the optimum phase angle. To stop oscillation, the PSCA monitors the oscillation in the phase angle and terminates the perturb and observe algorithm when oscillation is detected. The PSCA will allow the perturbation in one direction only to prevent oscillation in the harmonic vectors. Here, the perturb and observe algorithm can be stuck in a local

minimum phase angle and fails to reach the global optimum angle. Figure 7.8 shows all possible combinations of phase angles for three converters. The first converter is a master carrier and two synchronized converters. The phase angle of converter two and three shown in Figure 7.8 (a) and (b), respectively, are incremented by a 30-degree step with a different sample time to cover all the search space. The change in the ripple magnitude is shown in Figure 7.8 (c).

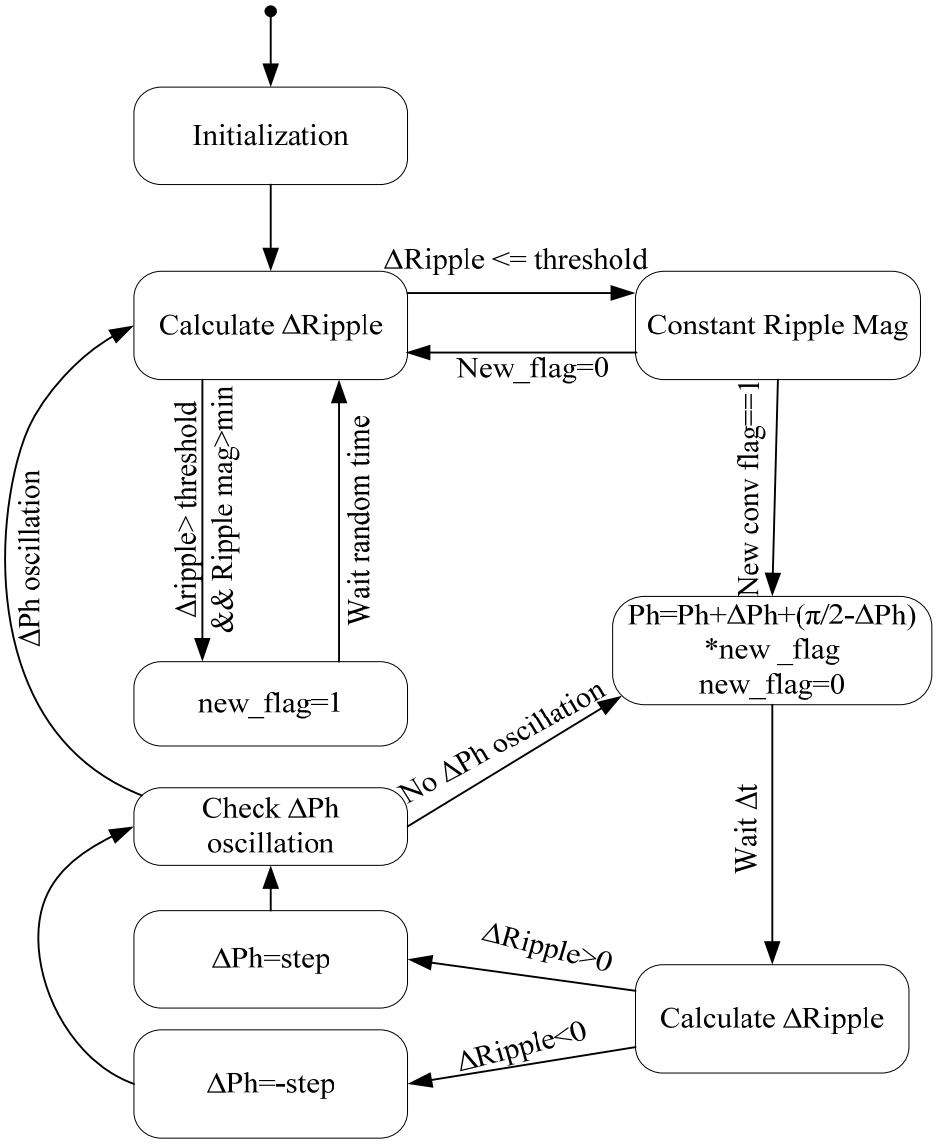


Figure 7.7: Search algorithm state machine

As depicted from Figure 7.8 to avoid stuck at the local minimum value, the initial perturbation should greater than or equal $\frac{\pi}{2}$ then increment with small step. PSCA will adjust the increment step to $\frac{\pi}{2}$ when the new flag is set and then change it to a regular increment step.

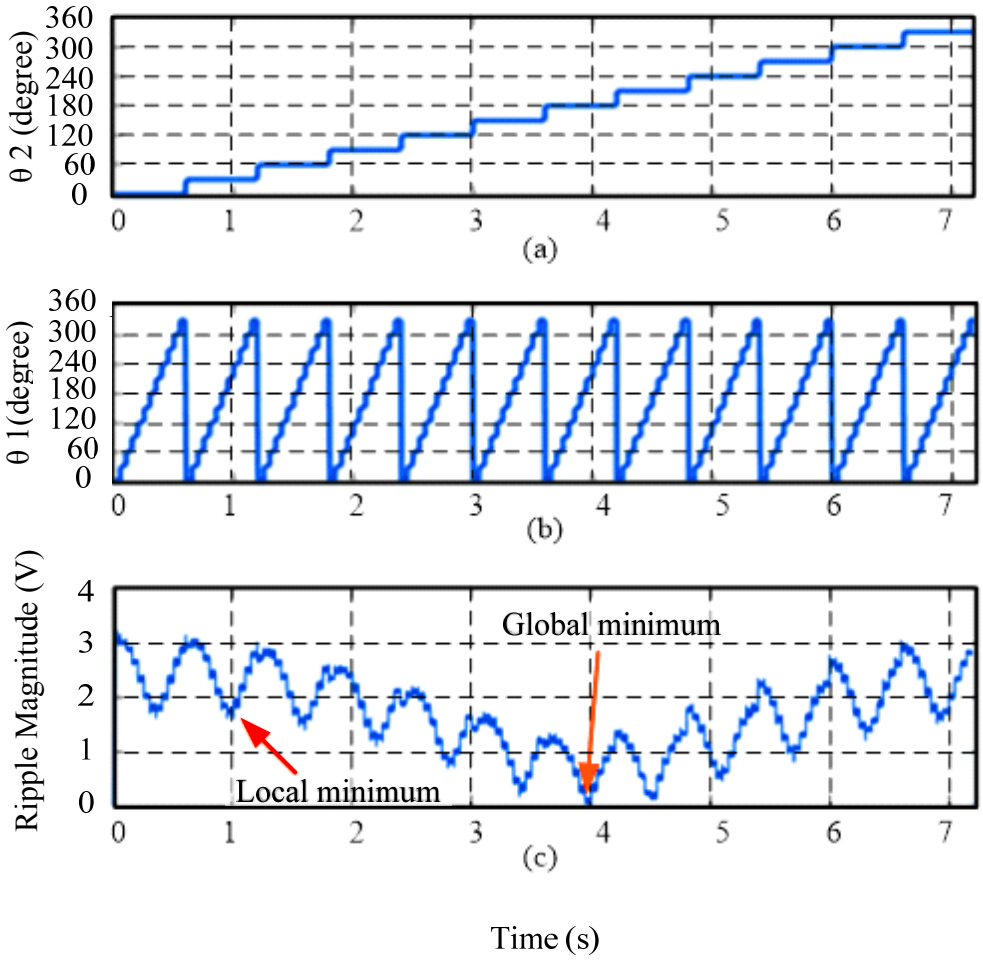


Figure 7.8: Perturb and observation search space

7.5 Simulation results

A model for three parallel converters, synchronization algorithm, and PSCA is built based on MATLAB/SIMULINK® to test and validate the robustness of the proposed

methods. The converters connection topology and parameters are shown in Figure 6.1 and Table 6-1in the previous chapter. All voltage and current controllers are identical to the controllers used with the GPS synchronization algorithm.

Two cases were simulated to validate the proposed methods under different operation conditions. The first case is for equal sharing load. In this case, 4 Ohm load was fed equally from the three converters with DC bus regulated at 40V and load current 10 A. However, in the second case, the master converter supplies 50% of the load demands while the two slave converters supply 25% of the load demands each.

7.5.1 Case one result

The simulation result for case 1 is shown in Figure 7.9. Figure 7.9-a, b, c, and d show the DC bus voltage, the ripple magnitude, converter 2 phase offset, and converter 3 phase offset, respectively. Initially, until around the first second, all converters start with a zero phase angle for the carriers. At t = 1.1 sec, the PSCA for converter 2 starts to search for the optimum phase angle and reaches 180 degrees. At this point, the PSCA detects a phase oscillation and terminates the search. During this period, the PSCA for converter 3 is sensing an amplitude change in the voltage ripple and thus remains idle. After the DC voltage ripple amplitude reaches its constant state, the PSCA for converter 3 starts to search for the optimal phase angle at t = 2 seconds. The PSCA for converter three stops its search when the perturb and observation algorithm reverses the perturbing direction to prevent oscillation in the harmonic vector and reaches phase angle equal to 30 degrees. Similarly, during the second period, the PSCA for converter 2 remains idle till the magnitude of the DC voltage ripple stabilizes again. After a random time period, the

PSCA for converter 2 repeats the same steps and stops at a 240 degrees phase shift, whereas the PSCA for converter 3 stops at 120 degrees. During the entire process, the PSCA are commanded to terminate the search algorithm when the DC voltage ripple falls below 0.5 V. In this simulation, the DC voltage ripple reached a minimum of 0.47 V. Figure 7.10-a, b, c, and d shows the phase angle between carriers during the search periods.

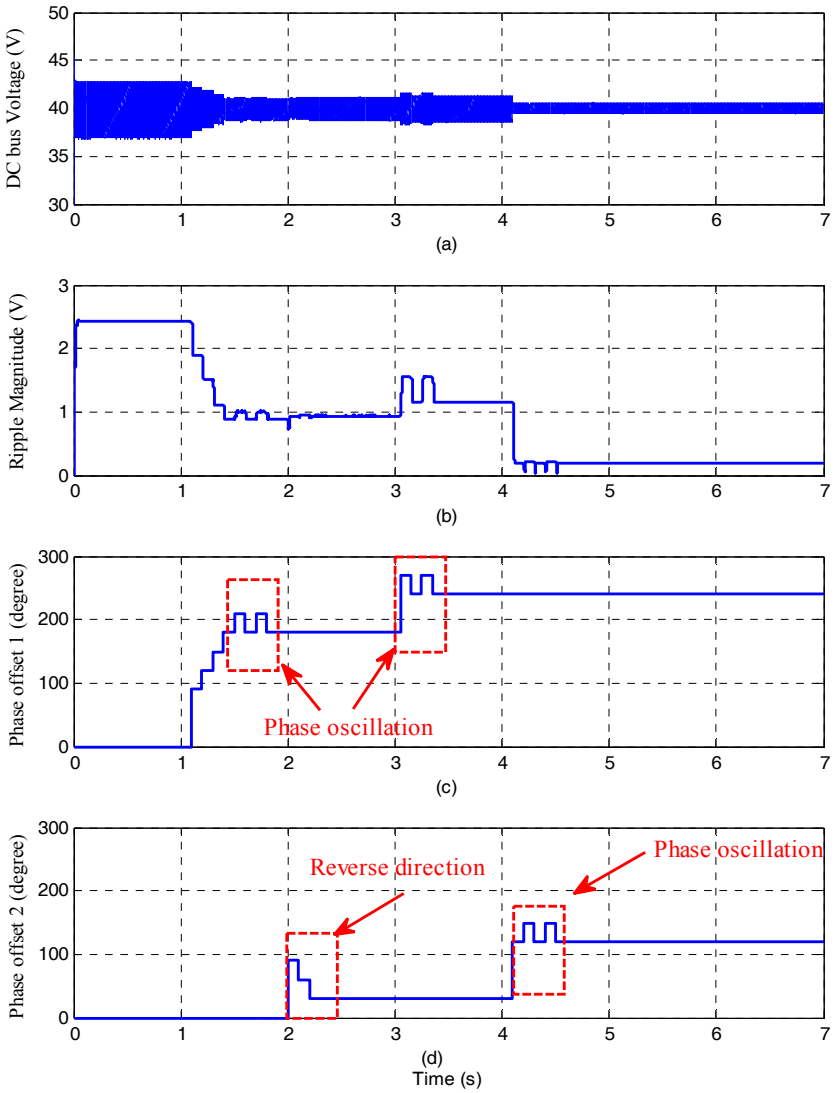


Figure 7.9: Case1 simulation results for Equal load sharing. (a) DC bus voltage ripple, (b) Ripple Magnitude, (c) Phase offset1, (d) Phase offset 2

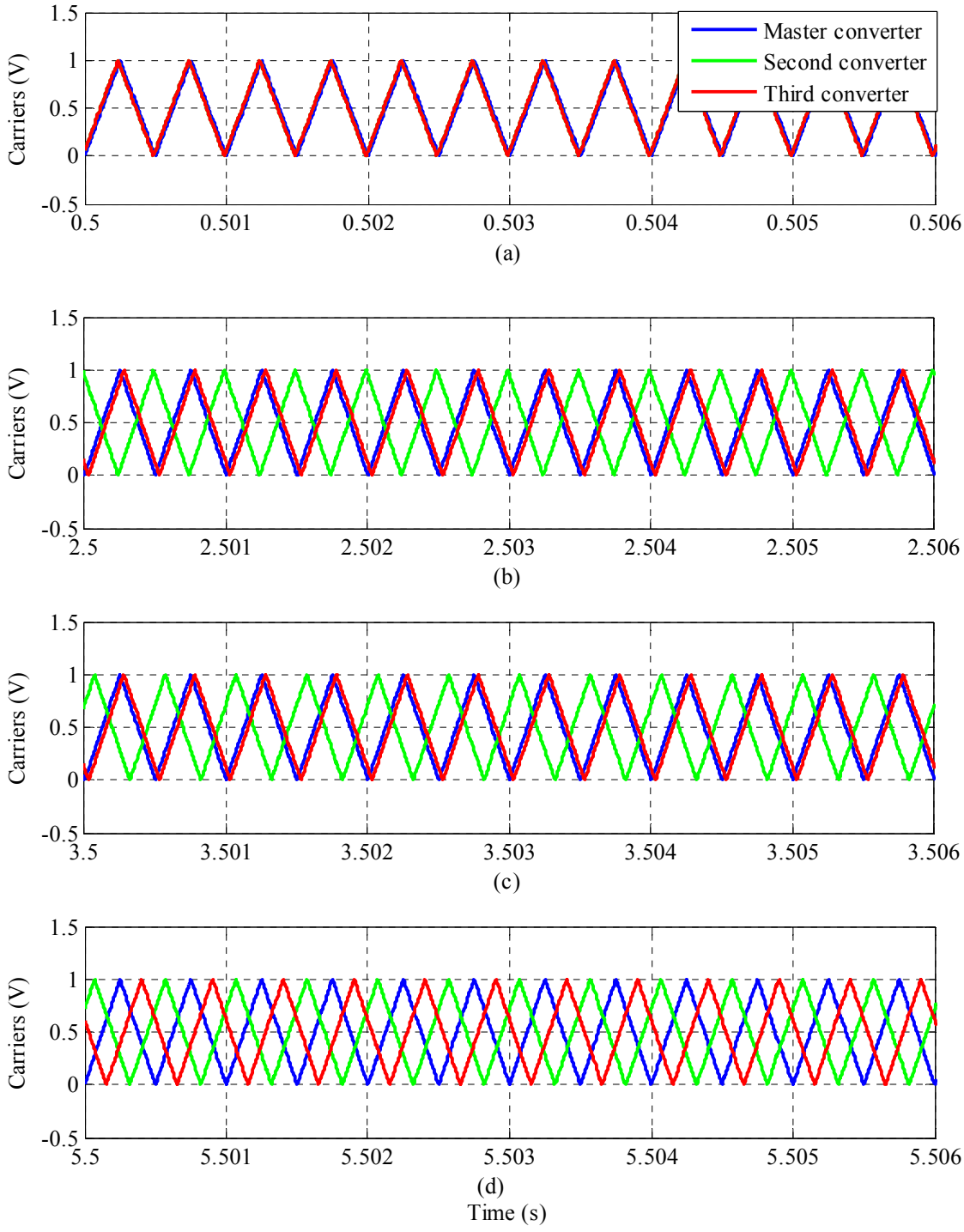
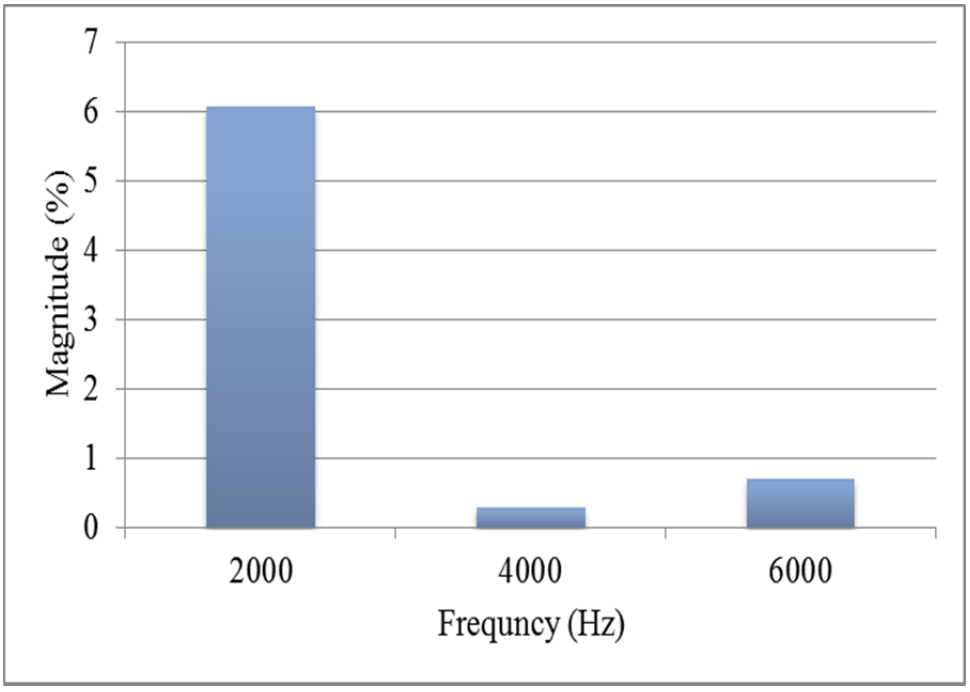
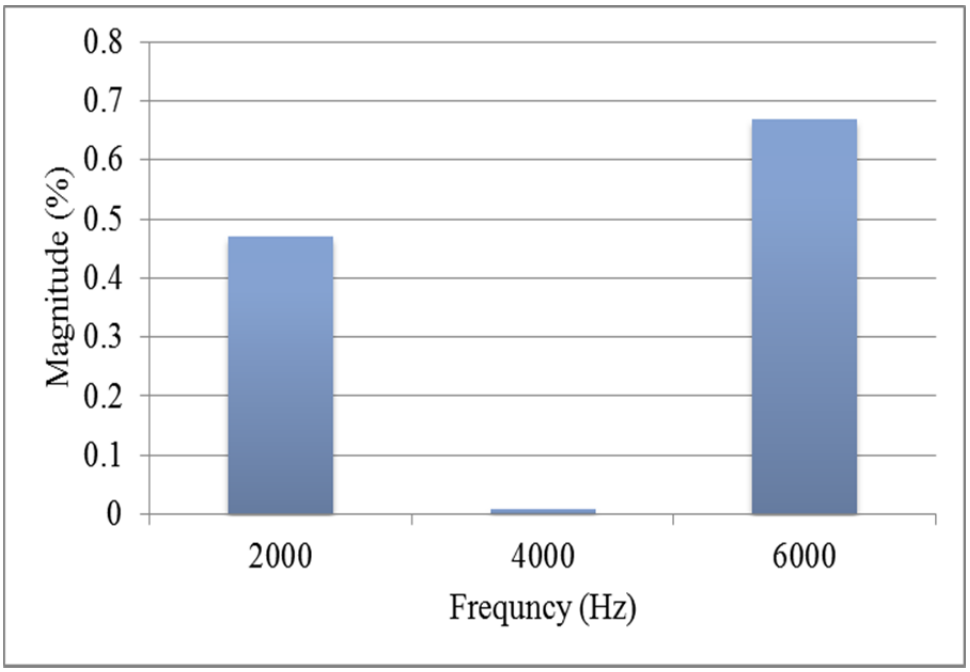


Figure 7.10: carriers phase angle for case one. (a) Carriers at t=0 s, (b) Carriers at t=2.5 s, (c) Carriers at t=3.5 s, (d) Carriers at t=5.5s



(a)



(b)

Figure 7.11: harmonics analysis for case 1. (a) Harmonics magnitude before PSCA, (b) Harmonics magnitude after PSCA

Harmonic analyses were performed for the DC voltage before and after applying the PSCA algorithm and the results are shown in Figure 7.11-a and b, respectively. As can be appreciated from the figure, the ripple component with the same frequency as the switching frequency (2000 Hz) was reduced significantly from 6.07% to 0.47%. The ripple for the 4000 Hz and 6000 Hz decreased in their turn from 0.29% to 0.01% and from 0.71% to 0.67%, respectively.

7.5.2 Case two: none equal Load sharing.

The simulation result for case 2 is shown in Figure 7.12. Figure 7.12 (a), (b), (c), and (d) show the DC bus voltage, the ripple magnitude, converter 2 phase offset, and converter 3 phase offset, respectively. Initially, until around the first half second, all converters start with a zero phase angle for the carriers. At t = 0.6 sec, the PSCA for converter 2 starts to search for the optimum phase angle and reaches 180 degrees. At this point, the PSCA detects a phase oscillation and terminates the search. During this period, the PSCA for converter 3 is sensing an amplitude change in the voltage ripple and thus remains idle. After the DC voltage ripple amplitude reaches its constant state, the PSCA for converter 3 starts to search for the optimal phase angle at t = 1.5 seconds. The PSCA for converter 2 stops at a 240 degrees phase shift. During the entire process, the PSCA are commanded to terminate the search algorithm when the DC voltage ripple falls below 0.5 V. In this simulation, the DC voltage ripple reached a minimum of 0.36 V. Figure 7.13 (a), (b), (c), and (d) shows the phase angle between carriers during the search period. Harmonic analyses were performed for the DC voltage before and after applying the PSCA algorithm and the results are shown in Figure 7.14 (a) and (b), respectively.

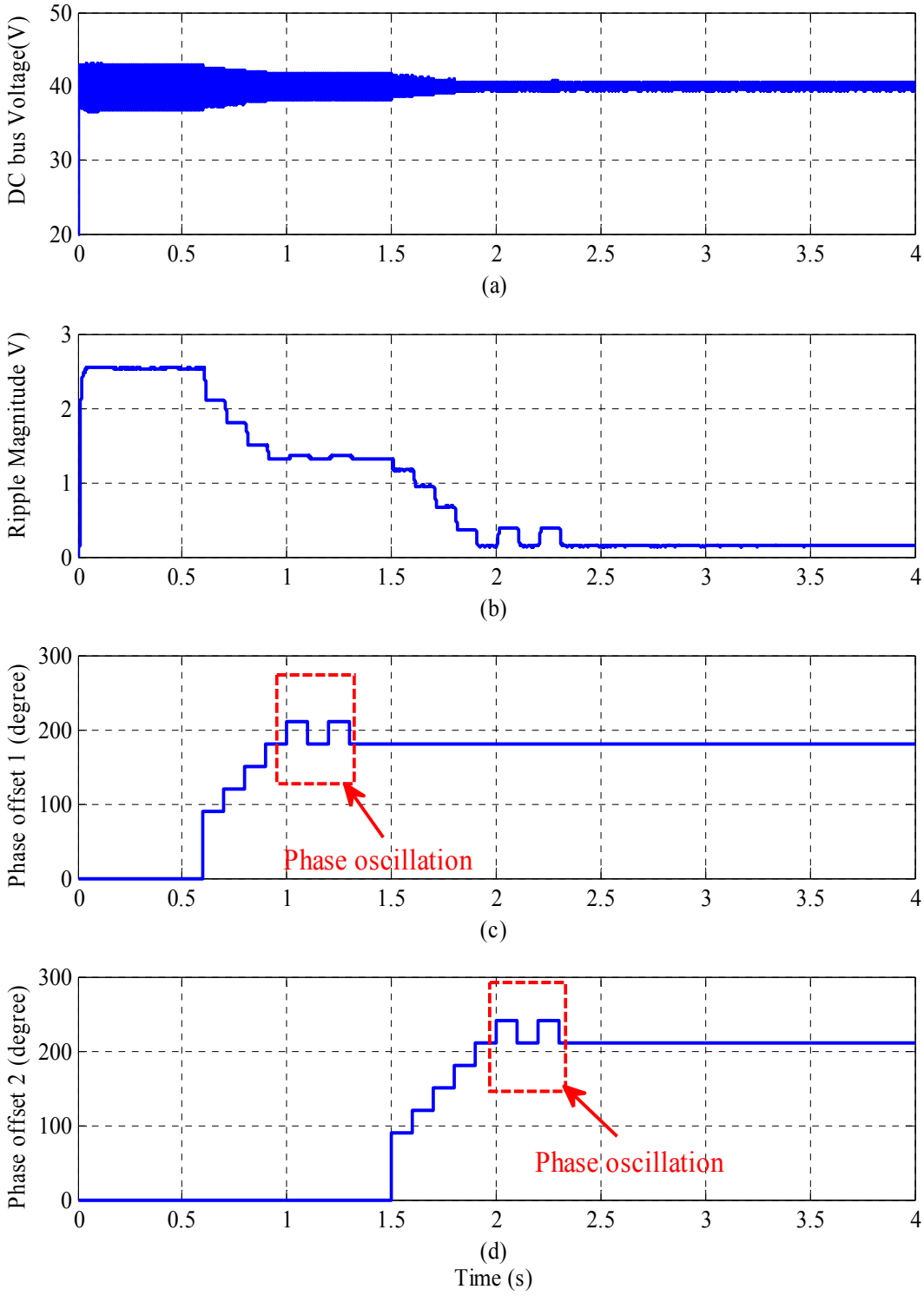


Figure 7.12: Case2 simulation results. None Equal load sharing. (a) DC bus Voltage, (b) Ripple Magnitude, (c) Phase offset 1, (d) Phase offset 2

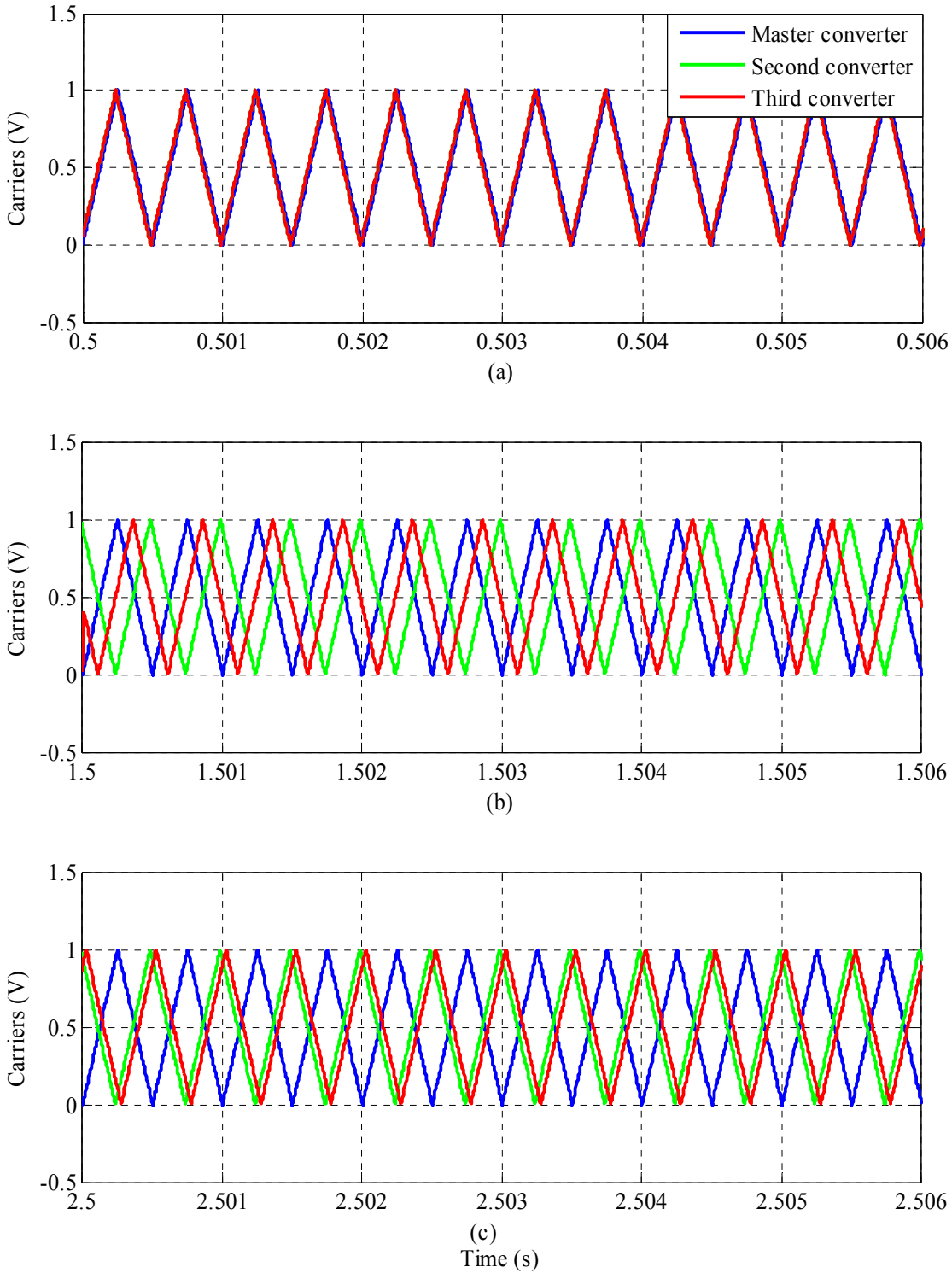
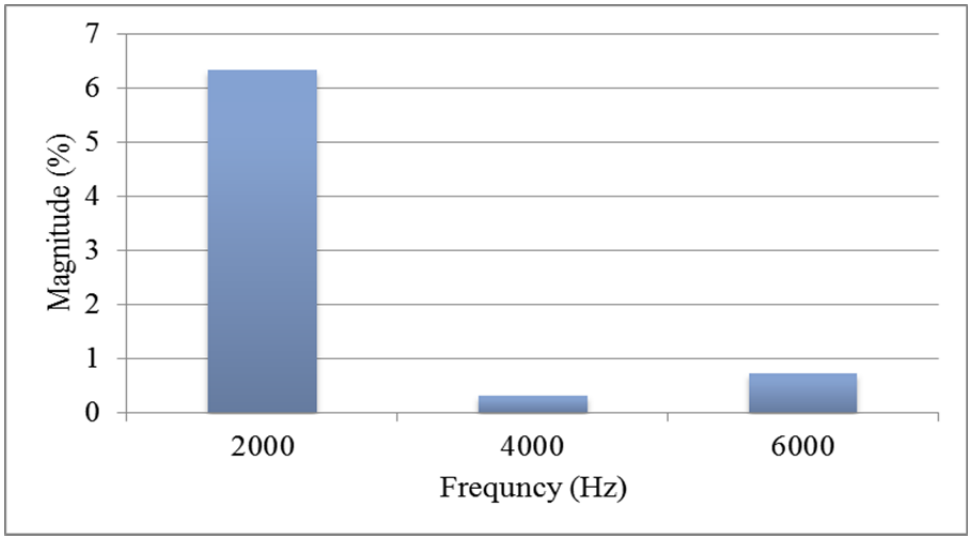
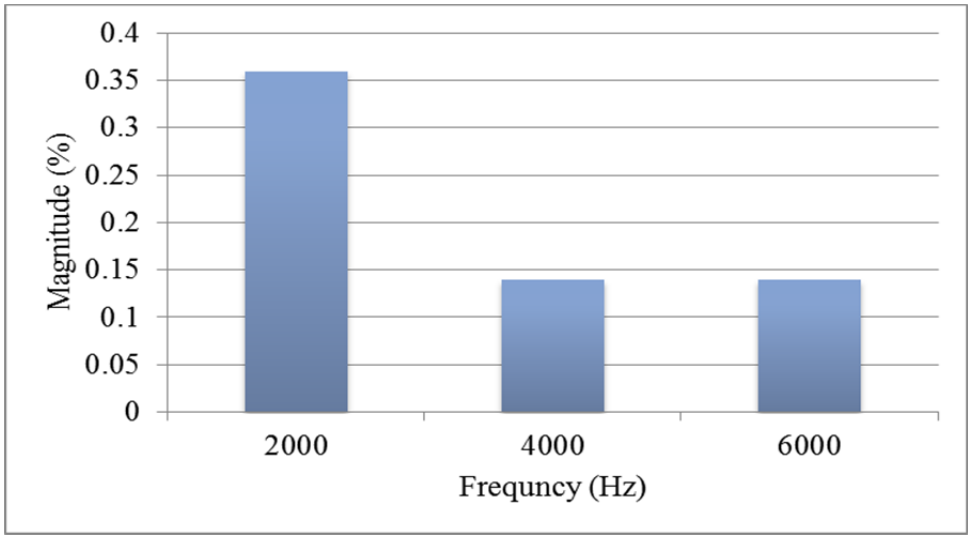


Figure 7.13: carriers phase angle for case two. (a) Carriers at t=0.5 s, (b) Carriers at t=1.5 s, (c) Carriers at t=2.5 s



(a)



(b)

Figure 7.14: harmonic analysis for case 2. (a) Harmonics magnitude before PSCA, (b) Harmonics magnitude after PSCA

As can be appreciated from the figure, the ripple component with the same frequency as the switching frequency (2000 Hz) was reduced significantly from 6.33% to 0.36%. The ripple for the 4000 Hz and 6000 Hz decreased in their turn from 0.31% to 0.14% and from 0.73% to 0.14%, respectively.

7.6 Hardware verification and experimental result

In order to implement the proposed algorithm in real-time, an experimental test bench, shown in Figure 7.15, has been designed. In this implementation, the ARM Cortex M4 Microcontroller is used to implement the functions of the carrier extraction, PSCA, and PWM. This control layer performs fast computation for the proposed algorithms and hard-real-time input/output function to control the DC-DC converters' semiconductor switches. The DSP extension for the ARM Cortex M4 assists in the fast computation of the control output. The built-in dedicated analog to digital converters with direct memory access makes it possible to acquire analog feedback signals with a fast sampling rate (100K sample /s). The STM32f407vgt6 32 Bit ARM cortex M4 processor running at 160MHz was used for the embedded implementation of the proposed algorithm.

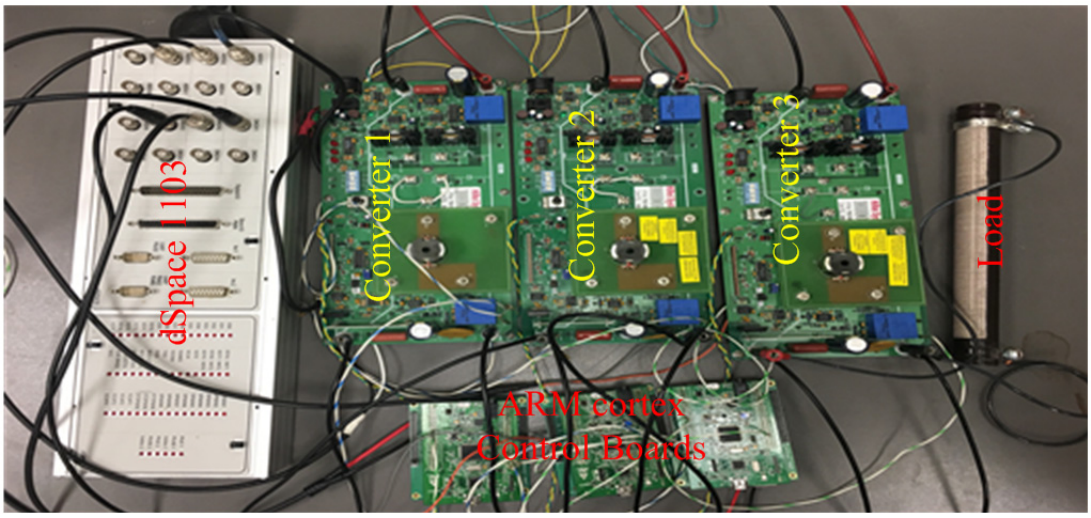


Figure 7.15: Hardware setup for carrier extraction and PSCA verification

To reduce the processing overhead and reach the sampling time of 1e-5 second, the PLL was replaced by frequency and phase estimator shown in Figure 7.16. The estimator calculates the frequency from the measured period between two zero crossing instances.

A digital integrator is used to calculate the phase angle from the frequency value. The digital oscillator is synchronized with the positive zero crossing signal to ensure that the calculated phase angle is synchronized with the carrier phase angle. The embedded firmware is generated from the Simulink model and compiled using the GNU C cross-compiler for ARM.

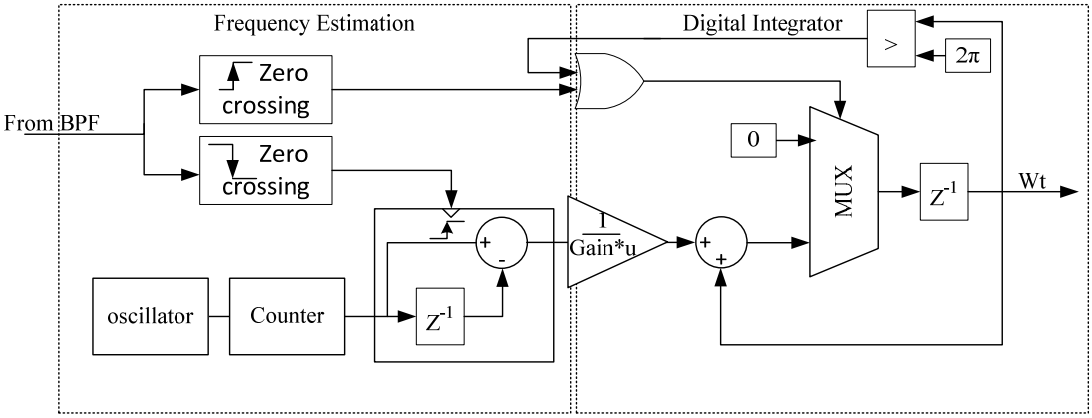


Figure 7.16: Low processing overhead frequency and phase estimator

The voltage and current control loops are implemented in dSpace 1104 embedded controller. The duty cycle reference is transferred from dSpace to the ARM processor as an analog reference. The embedded code in the ARM processor compares received duty cycle with the internal carrier and generates PWM digital output to drive the DC-DC boost converter. The power circuits for the three converters have the same parameter and topology used in chapter 7 experiment. The three converters are connected to the 4 Ohm load and 40 V common DC bus. The controllers for the three converters are adjusted to equally share the load current.

Figure 7.17 and Figure 7.18 show the DC bus voltage during PSCA search and finale carrier phase angle, respectively. As depicted from figure 17, the proposed algorithm reduces the ripple magnitude from 3 V to 0.75 V with optimized carrier phase angle.

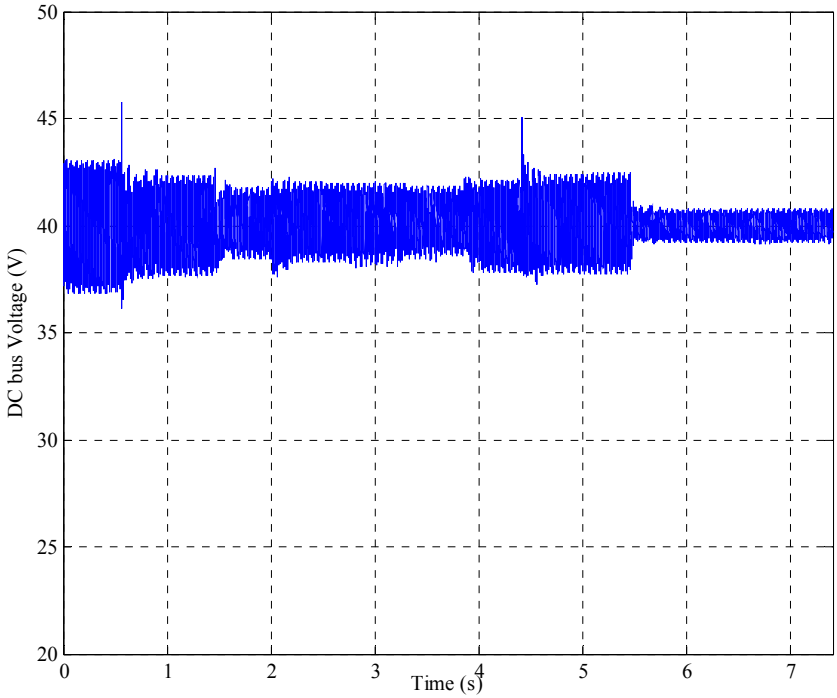


Figure 7.17: DC bus voltage with PSCA.

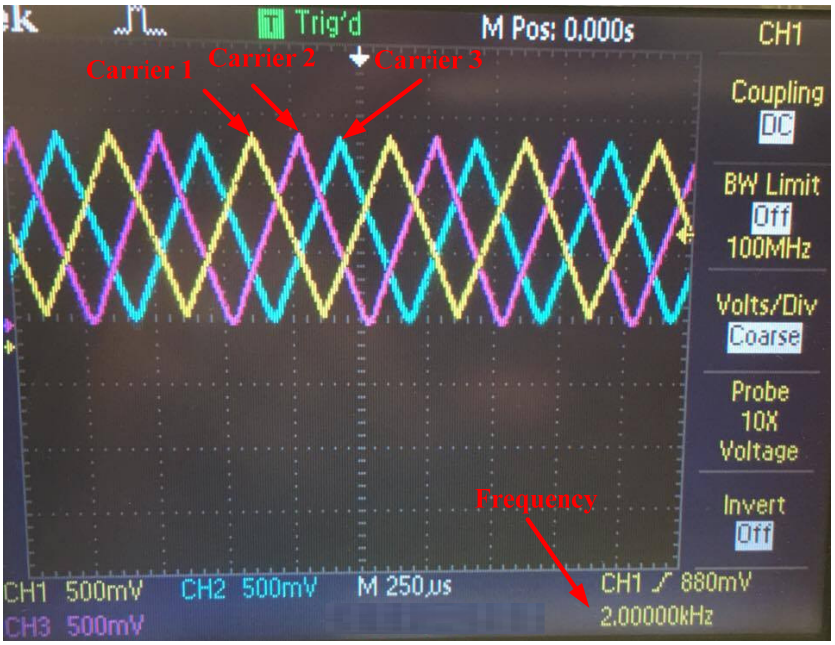


Figure 7.18: Three converter carriers after PSCA

7.7 Summary

In this chapter, a new synchronization and PSCA for PWM carriers of DC-DC converters based on carrier extraction is proposed. The advantage of this synchronization method is that it does not require a GPS time reference. Therefore, it eliminates the risk of GPS spoofing attacks. Simulation results on a multiple converter system showed the success of the proposed synchronization method in minimizing the DC bus voltage ripple to below 0.5 V. Finally, experimental results showed the excellent performance of the proposed method.

Chapter 8 Microgrid Inverter Based Synchronization and Islanding Detection

8.1 Introduction

The increased adoption of new energy sources and distributed generation (DG) is contributing to the continuous evolution of grid interconnection requirements towards a better control of generated power and enhanced contribution of distributed power generation systems to the overall power system stability. There is a great requirement for the ability of DG units to stay connected during short grid disturbances. In addition, this is needed to provide active/reactive power control at the point of common coupling[85]. Most renewable DG systems are connected to the grid through power electronics converters. The synchronization mechanism used to synchronize the power converter to the AC grid play a vital role in the performance of such systems during faults and transient conditions [85], [86]. The ability to stay connected under unbalanced or fault conditions and the sensitivity to voltage sag, voltage dip and harmonics are dependent on the synchronization mechanism[85].

The classical synchronization technique using zero crossing detection or charge pump phase locked loop (CP-PLL) fails under distorted voltage conditions [85], Synchronous Reference Frame phase locked loop (SFR-PLL) with low bandwidth shows good performance under distorted voltage conditions but it has slow response during transient and is sensitive to frequency fluctuation and unbalanced voltage [87].

For unbalanced condition, some PLL uses an all-pass filter (APF) to detect and isolate the negative sequence [88]. Most PLL techniques fail to provide stable frequency after

losing the grid frequency reference due to a grid disconnection. Maintaining stable frequency after a grid disconnection is very important for microgrid to continue its operation in islanding mode and feed the local AC loads. Implementation of islanding detection is imperative for the microgrid. Failure to detect islanding condition could cause safety hazards to the utility workers and equipment damage. Several techniques were introduced to detect islanding condition using active, passive and remote detection methods [89]. Passive islanding methods monitor voltage, the active and reactive power to detect an islanding condition. Passive detection fails when local load and energy produced by the microgrid are balanced. Active methods inject small signals, such as high frequency or negative sequence components, into the line and detect signal changes [89]. The active detection method provides a robust islanding detection solution but it uses complex algorithms for current injection and detection of changes. The Remote detection method solution relies on communication signals, such as power line carriers PLC communication, remote disconnect signals, and SCADA systems in addition to PMU- based islanding detection[90]. The remote detection method is prone to communication failure problems. Losses of PLC carrier or communication with the SCADA system could lead to false islanding detection and disconnection of the microgrid.

In this chapter, an accurate synchronization technique based on adaptive SRF-PLL (ASRF-PLL) under unbalanced and distorted voltage condition is introduced moreover the proposed ASRF-PLL is able to detect islanding condition and switch to stable frequency during standalone operation and automatic resynchronization with the grid

when it became available. The islanding detection signal from ASRF-PLL can be used to reconfigure the grid tie converter control to work in voltage control mode during standalone operation or power control mode during grid connection. The proposed ASRF-PLL is completely software based, which can be implemented in digital processors which eliminate the errors caused by component drift in hardware based solutions. The superior performance and unique features of the proposed PLL increase the Microgrid stability and reliability. A reconfigurable controller for the grid-connected converter was also introduced to work in conjunction with the PLL to ensure proper operation in islanding mode.

8.2 Conventional SRF-PLL

The SRF-PLL concept is based on aligning the output frequency of the controlled oscillator with the d axis in the dq frame by forcing the q component to be zero using a PI controller. Refer to Figure 8.1, which shows the basic structure of the SRF-PLL.

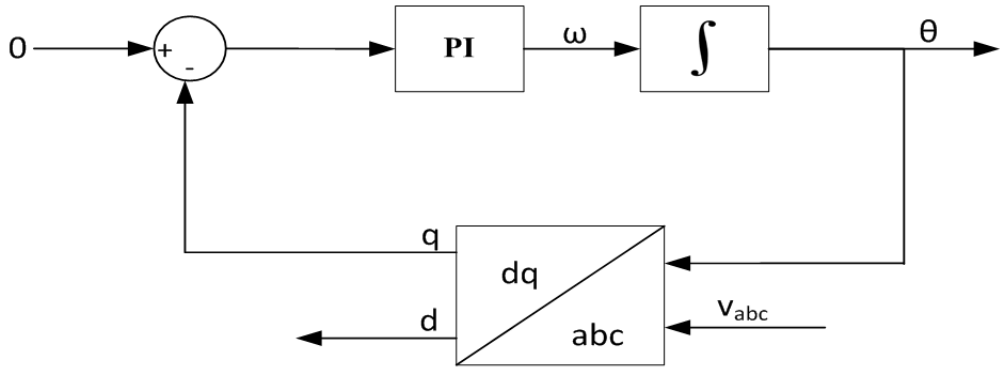


Figure 8.1: Conventional SRF-PLL

The three-phase voltages V_a, V_b, V_c, are transferred to synchronous reference frame using Park's transform and estimated phase angle θ equation (8.1).

$$\begin{bmatrix} v_d \\ v_q \\ v_0 \end{bmatrix} = \frac{2}{3}\begin{bmatrix} \sin(\theta) & \sin\left(\theta - \frac{2\pi}{3}\right) & \sin\left(\theta - \frac{4\pi}{3}\right) \\ \cos(\theta) & \cos\left(\theta - \frac{2\pi}{3}\right) & \cos\left(\theta - \frac{4\pi}{3}\right) \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{bmatrix}\begin{bmatrix} v_a \\ v_b \\ v_c \end{bmatrix} \quad (8.1)$$

Now, the PI controller forces the v_q component to become zero to align the PLL output with the d axis. When the PLL output becomes in phase with the supply voltage, the PI output will be equal to the angular frequency ω and θ can be obtained by integrating the PI output. Assuming clean and balanced voltage, a DC component only will exist in the dq axis; the PI controller will force this DC value to become Zero in the q axis. In the case of the unbalanced voltage, an AC component with a frequency equal to twice the supply frequency will exist in the dq axis. This AC component will cause oscillation in the estimated frequency and phase angle. This error in estimating phase angle can lead to injecting a harmonic current to the supply system and power oscillation. Harmonic voltage also causes an AC component in the dq axis with orders equal (n-1), where n is the harmonics order in the abc frame. Figure 8.2 shows the effects of unbalanced voltage on the stability of SRF-PLL. Unbalanced voltage due to external fault could lead to large oscillation in the SRF-PLL output frequency. The frequency oscillation could force the protection system to disconnect the microgrid from the utility. Disconnecting microgrids during faults will increase the stress on the utility due to losses of DG resources. The impact of harmonic on the SRF frequency estimation is shown in Figure 8.3. The presence of the fifth harmonic with 5% magnitude causes an oscillation in the SRF_PLL frequency output.

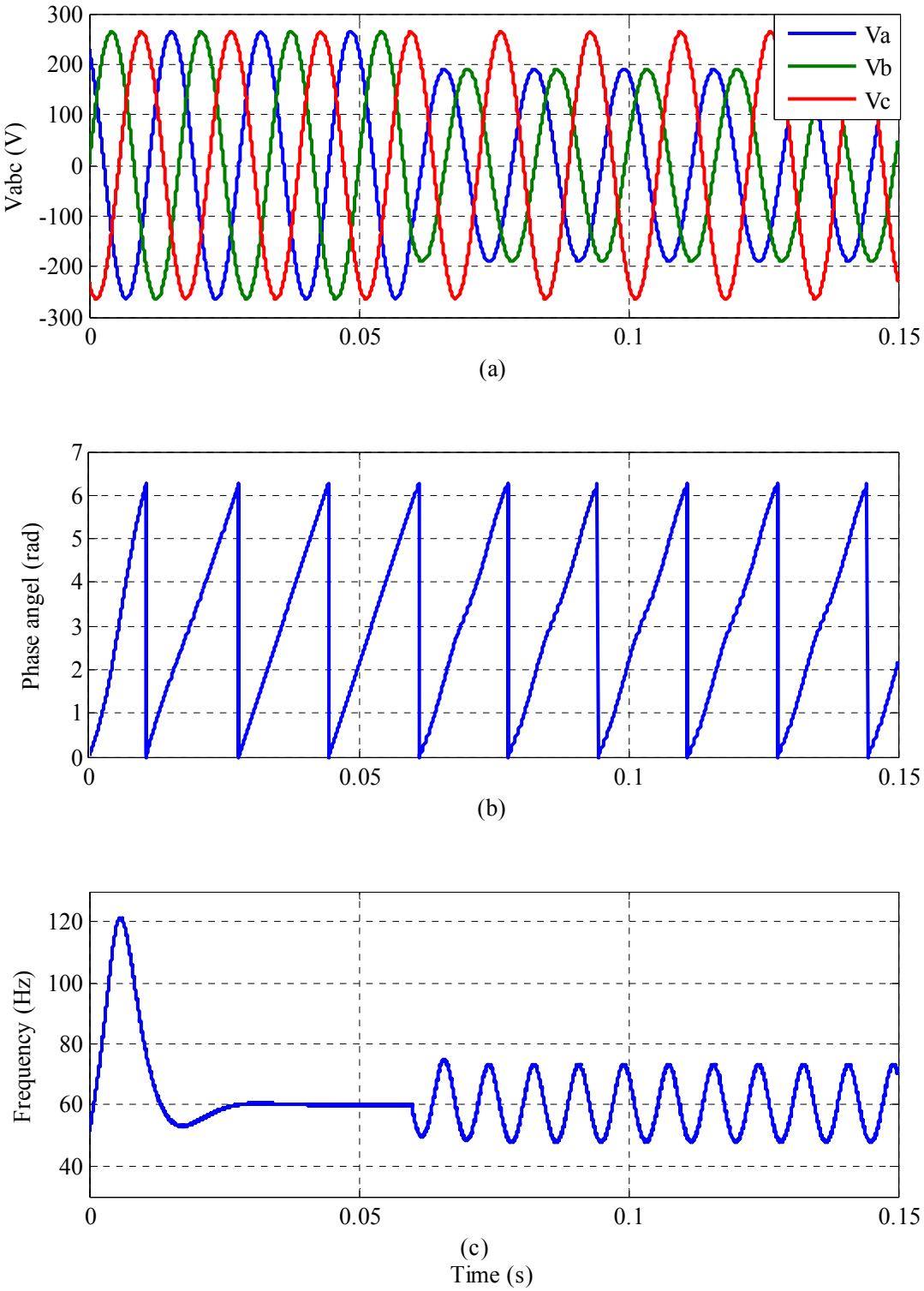


Figure 8.2: SRF-PLL Phase angle and estimated frequency under unbalanced voltage condition. (a) Three phase voltage. (b) Phase angle. (c) Estimated frequency

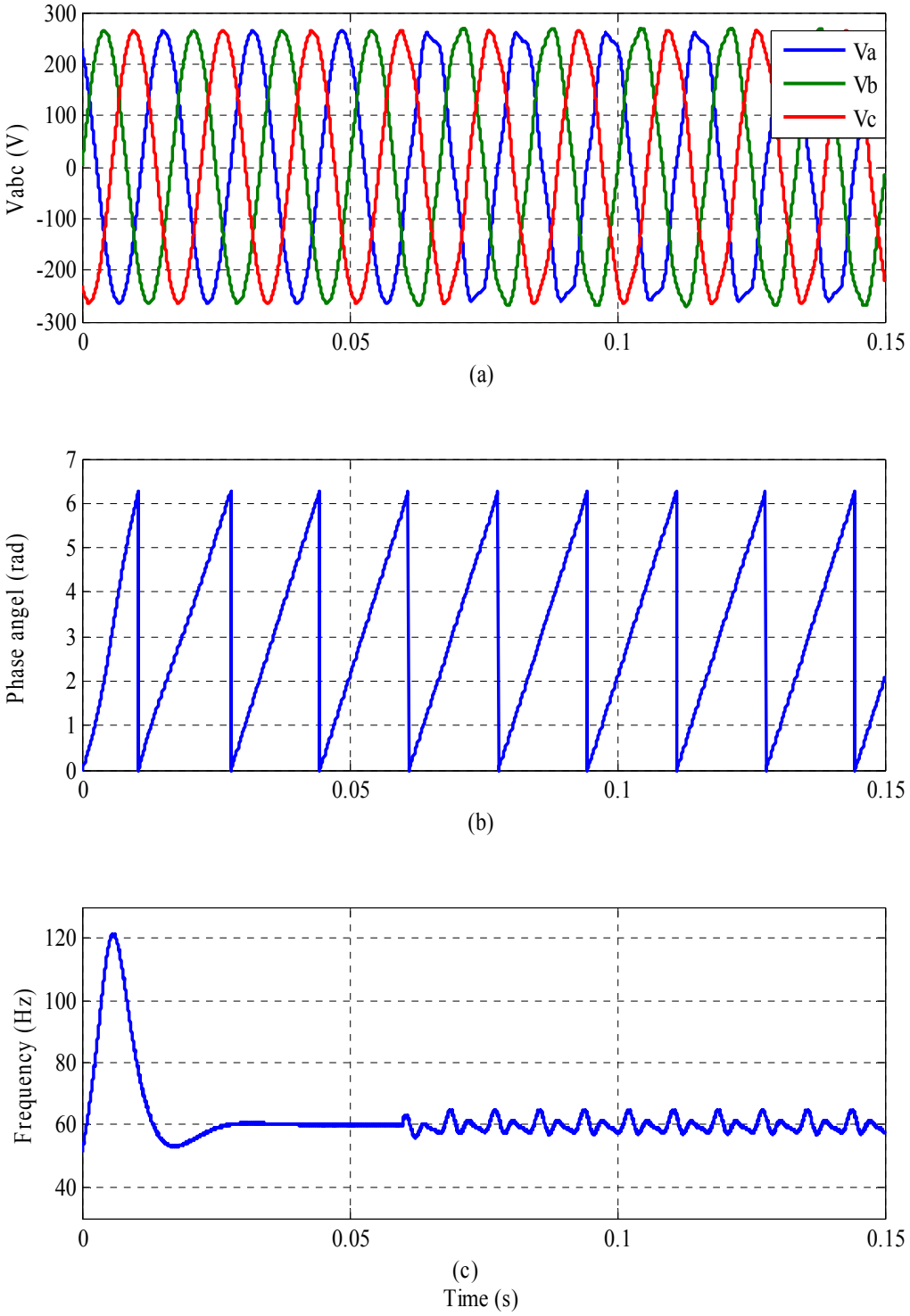


Figure 8.3: SRF-PLL Phase angle and estimated frequency under distorted voltage condition. (a) Three phase voltage. (b) Phase angle. (c) Estimated frequency

8.3 Adaptive SRF-PLL

To improve the performance of the conventional SRF-PLL, the AC component associated with the harmonic and unbalanced condition must be rejected. To reject the AC component in the dq synchronous frame, a traditional low-pass filter with cut-off frequency < 2ω is used. A high order filter is also required to obtain high attenuation for the AC components. This type of filter will lead to a poor transient response. The proposed technique uses an adaptive moving average filter to reject the AC components resulting from harmonics and unbalanced voltage without affecting the transient performance of the PLL.

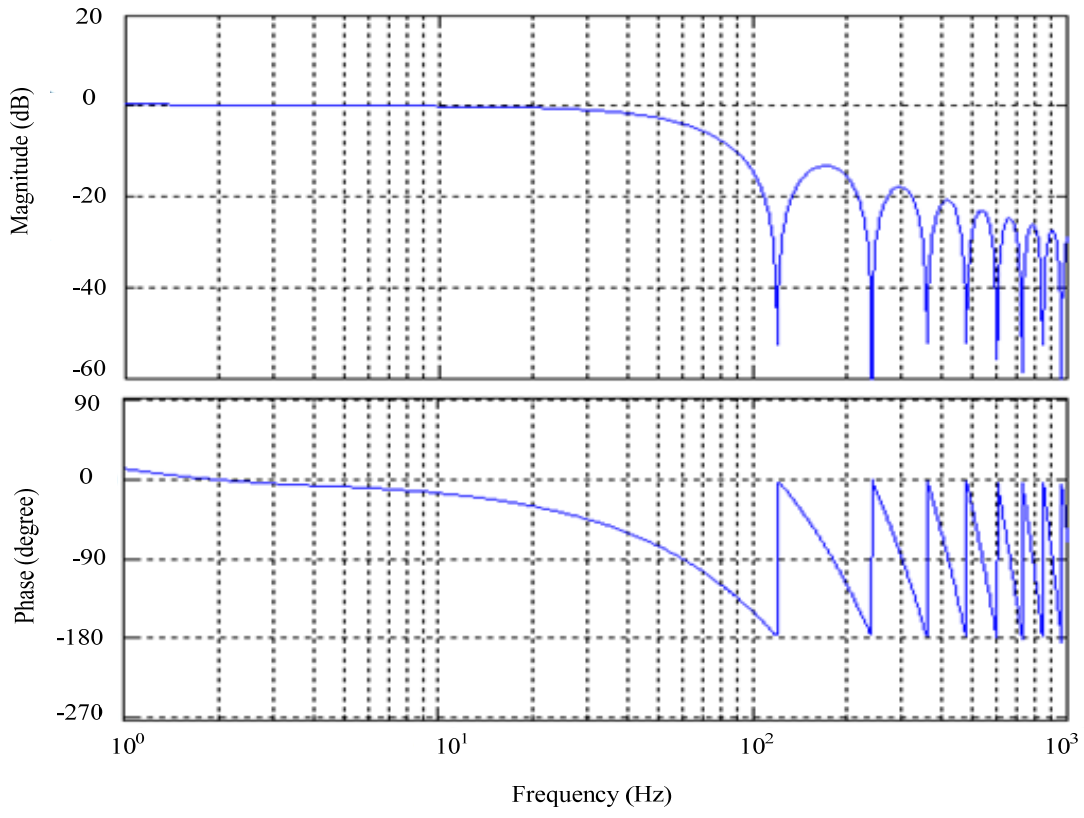


Figure 8.4: Moving average filter frequency response

Moving average filter is a type of finite impulse response filter (FIR), which creates a series of averages of sampled signals over a defined window. If the moving average filter runs with a window size of 1/120 sec, it will be able to reject the signal with 120 Hz and its integral [91]. Since the AC components in the dq frame are always even and always integral of 120Hz in a 60Hz supply system and are also an integral of 100Hz in a 50Hz supply system, then the moving average filter will be able to reject all ripples resulting from harmonics and unbalanced voltage. Figure 8.4 and Figure 8.5 shows a frequency response comparison between the moving average filter with average window equal 1/120 sec and second-order Butterworth low-pass filter with cutoff frequency 12Hz.

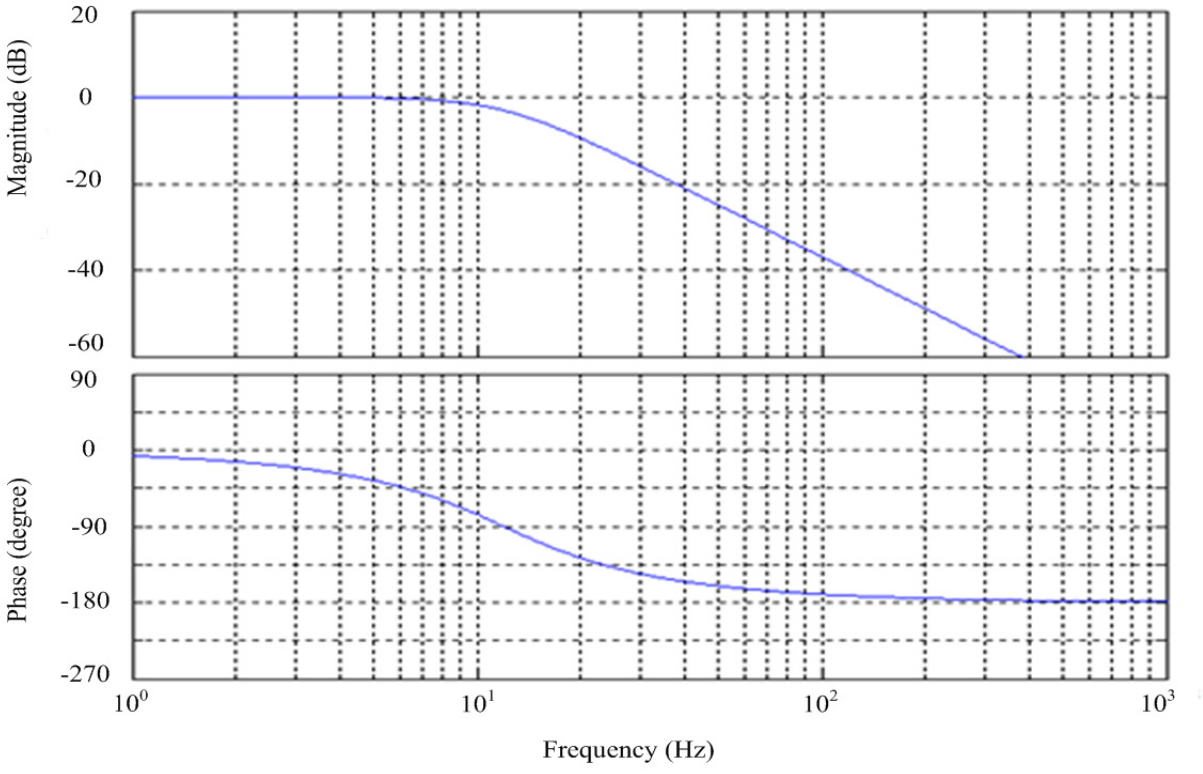


Figure 8.5: Butterworth low pass filter frequency response

Both moving average filter with 1/120 sec window and Butterworth low-pass filter with cutoff frequency of 12Hz have attenuation equal to 40dB at 120 Hz. The Butterworth filter has a phase margin equal to -135 degree at 20Hz and -164 deg at 60 Hz. However, the moving average filter has -45 degree at 20Hz and -90 deg at 60Hz. Also, the Butterworth low-pass attenuates all the frequency components with a frequency greater than 120 Hz, which slow down the PLL response, while the moving average filter attenuates only the component with a frequency equal to multiple of 120Hz.

In the weak grid that has multiple small generations with low inertia, the frequency might deviate from the nominal value. In this case, the performance of PLL with moving average filter tuned at fixed window will degrade due to change in the operating frequency. If the moving average filter has an adaptive window size that changed automatically according to the supply frequency, the filter will have the same attenuation for the AC component at the new operating points. The PLL will then be able to follow the frequency drift without any degraded performance. Figure 8.6 shows the SIMULINK model for proposed PLL with adaptive window size. The window size will always be equal to $\frac{1}{2*f}$, where f is the estimated supply frequency to ensure the attenuation of all AC component results from unbalanced and harmonics voltage

The performance of the ASRF-PLL is depicted in Figure 8.7 and Figure 8.8. The proposed method greatly improved frequency and phase estimation under distorted and unbalanced voltage condition. The moving average filter damps the frequency oscillation and improves phase detection accuracy.

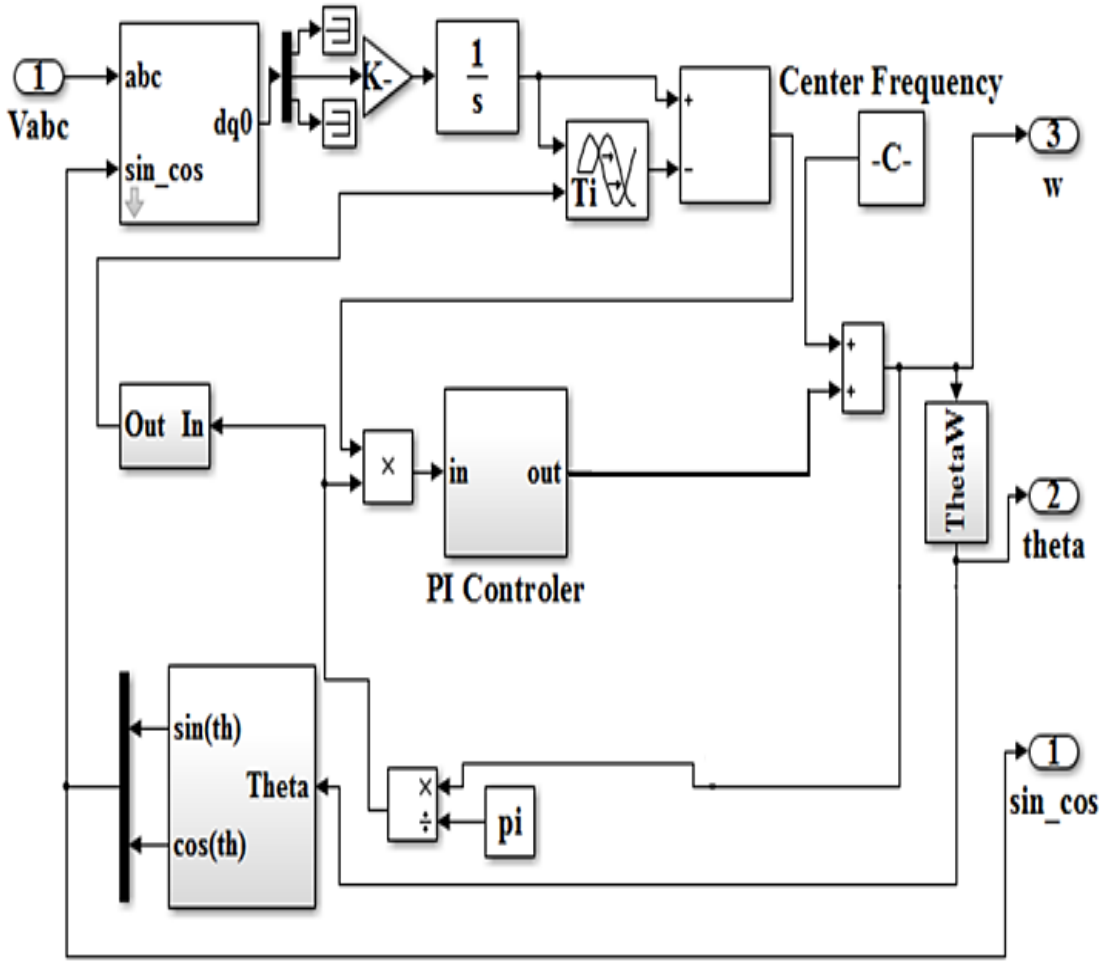


Figure 8.6 Proposed ASRF-PLL with an adaptive moving average filter simulation model

In Figure 8.7 an unbalanced voltage condition occurs at a time equal to 0.06 sec. The ASRF-PLL output frequency slightly fluctuated and restored back to 60 Hz in less than a quarter cycle. The estimated frequency is fixed at 60 Hz with no oscillation. The Same performance is obtained with distorted voltage condition. In Figure 8.8, at time equal 0.06 sec, 5% fifth harmonic is injected to the phase voltage. The ASRF-PLL succeeds to reject the harmonic frequency and produce stable frequency and phase angle references. It's worth to noting that the conventional SRF has 120 Hz overshoot during startup while the proposed method has 85 Hz overshoot.

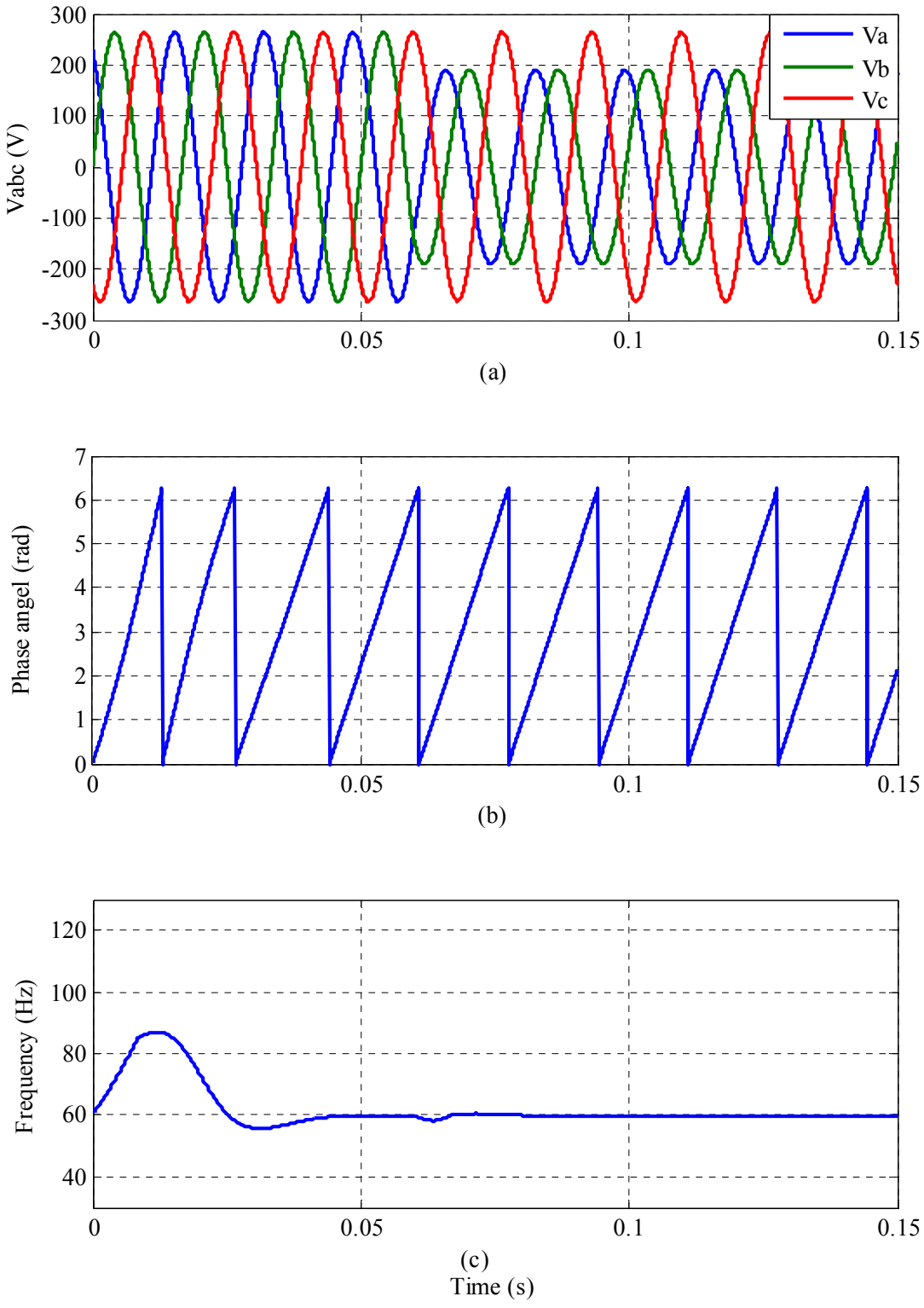


Figure 8.7: ASRF-PLL Phase angle and estimated frequency under unbalanced voltage condition. (a) Three phase voltage. (b) Phase angle. (c) Estimated frequency

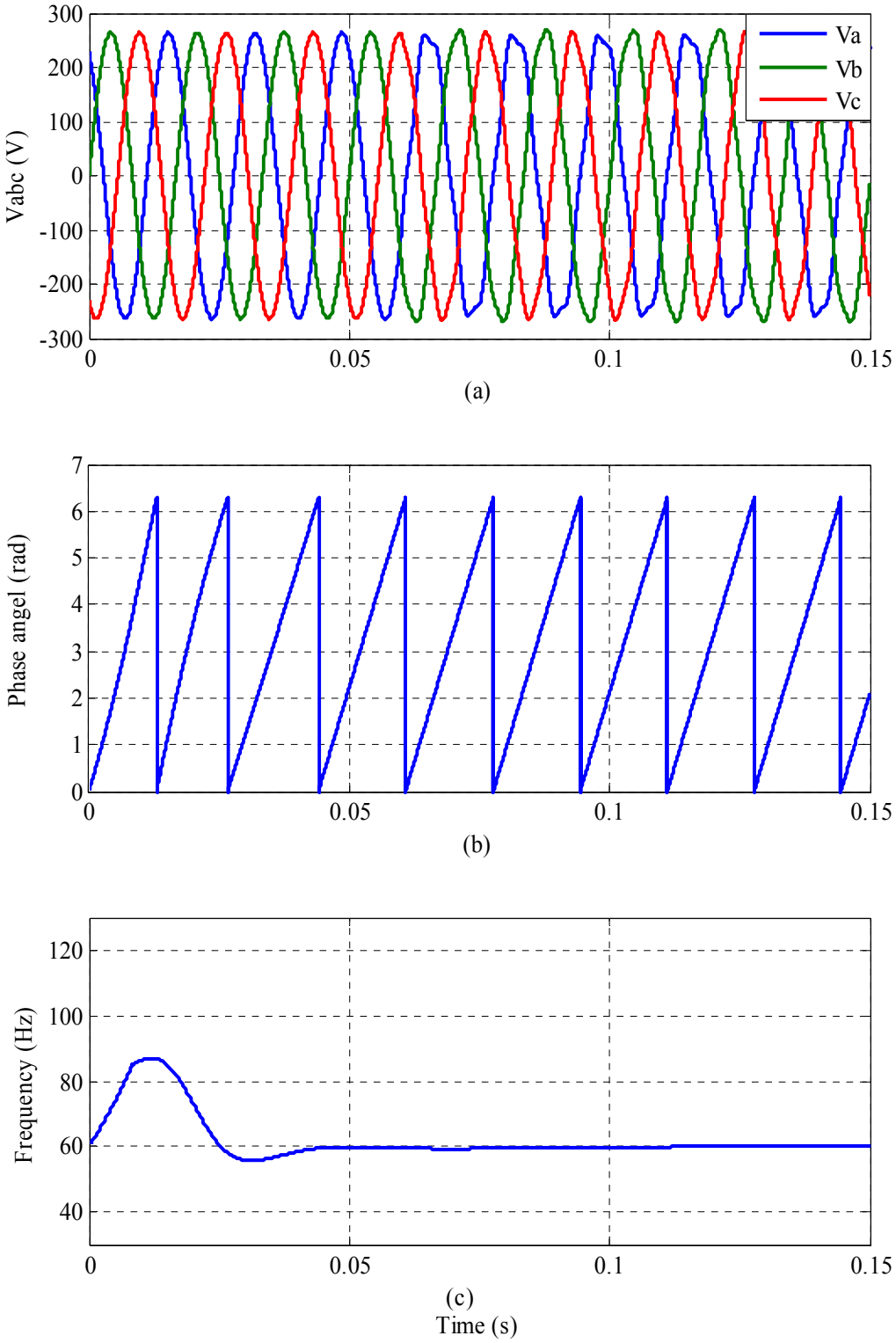


Figure 8.8: ASRF-PLL Phase angle and estimated frequency under distorted voltage condition. (a) Three phase voltage. (b) Phase angle. (c) Estimated frequency

8.4 Islanding detection and standalone operation

Most PLL techniques fail to maintain the frequency stability after sudden grid disconnection and introduce large frequency drift in the absence of the grid frequency reference in the Microgrid applications. It is necessary to maintain the frequency stability in islanding mode to prevent interruption of service and continue to feed the local loads with available power from the local distributed generation. To achieve this goal, a small error is introduced to the PLL center frequency. This error will be compensated by the PI controller in the presence of the grid frequency reference. In absence of grid frequency reference, the error will be accumulated and cause frequency drift in the PLL output. An islanding detection algorithm is implemented inside the PLL to detect the frequency drift in the PLL output after grid disconnection. The trip signal from the detection algorithm is used to trigger three important functions in the microgrid control system. First, the trip signal triggers the PLL to switch to internal frequency reference to maintain fixed and stable frequency. The second function of the trip signal is triggering the grid converter control to change the control mode from power control mode to voltage control mode. The last function of the trip signal is to trip the circuit breaker between the microgrid and the main grid. A reset signal from a voltage detector can be used to reset the PLL to switch back from internal reference and resynchronize with the grid when the main grid becomes available. Figure 8.9 shows the SIMULINK model for the proposed islanding detection algorithm. If the frequency drift becomes greater than the defined threshold for the defined time period the detection algorithm will trigger the trip signal. Figure 8.10 shows the proposed ASRF-PLL complete with adaptive moving average filter and islanding detection.

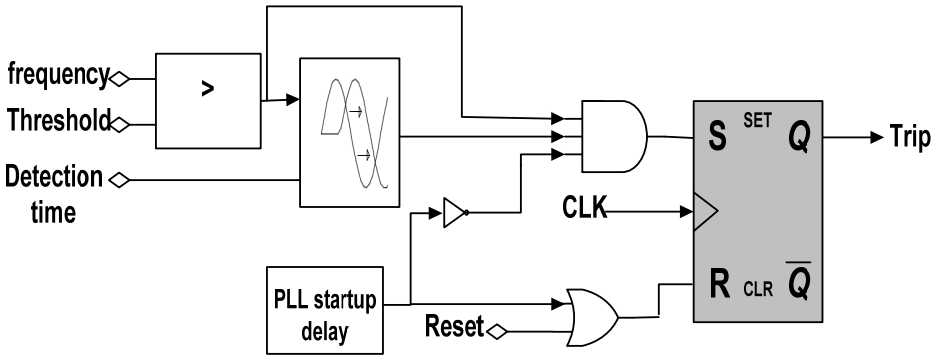


Figure 8.9: SIMULINK model for islanding detection algorithm.

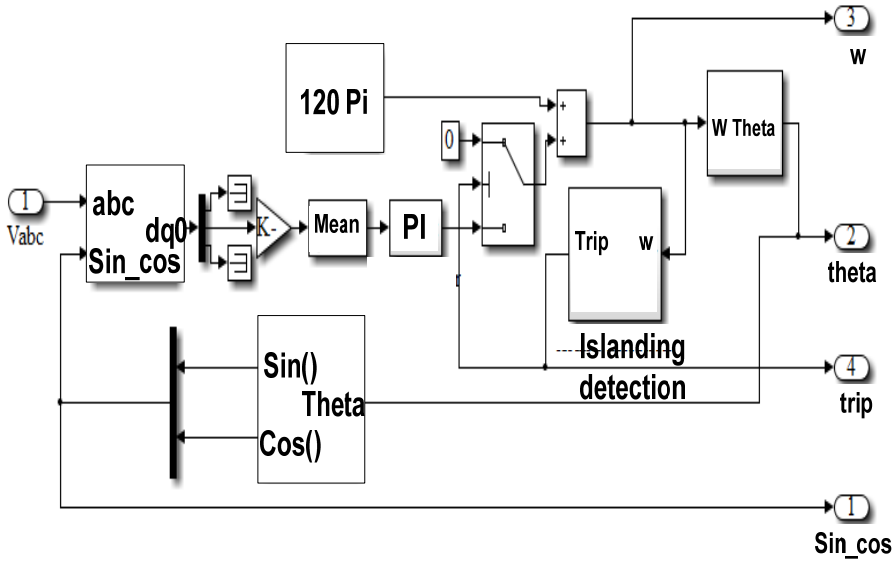


Figure 8.10: SIMULINK model for proposed ASRF-PLL with islanding detection algorithm and internal frequency reference

8.5 Microgrid control reconfiguration

Most distributed generation units in the microgrid are usually connected to the main grid using power electronics converters. In normal mode, the converters' controls are working in power control mode to control the power flow between the microgrid and the main grid. The voltage at the point of common coupling is regulated by the main grid. If

the grid is disconnected and the converter continues to work in power control mode, the voltage at the converter terminals will become unregulated. Feeding constant power after grid disconnection could lead to over voltage in the case when injected power exceeds the local load's demands. This situation can cause severe conditions to the Microgrid and interrupt the microgrid service. To improve the microgrid reliability and maintain continues service, the converter control must be automatically reconfigured for voltage control mode when islanding is detected, to regulate the voltage and continue feeding the local load. The reconfiguration process is triggered by the trip signal from islanding detection algorithm. Figure 8.11 shows the block diagram for the proposed reconfigurable converter control algorithm.

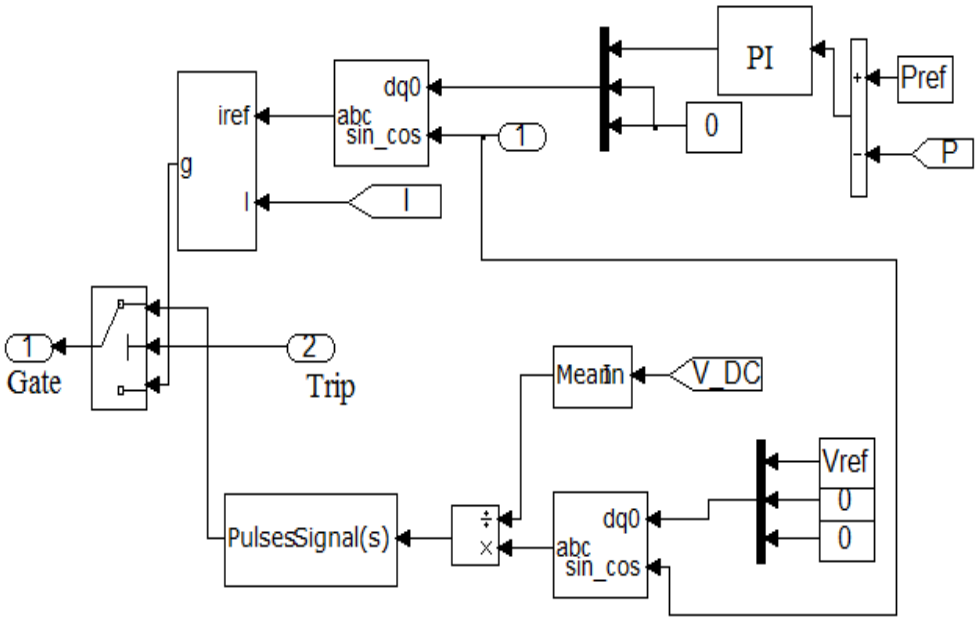


Figure 8.11: Reconfigurable converter control

The proposed controller consists of two sub-controllers. The first controller is power controller, which is implemented in the dq frame to control the active power. The power

reference is subtracted from the measured power and the error signal is fed to a PI controller to generate the reference current I_d in the dq frame. The I_d is transferred to the abc frame and fed to a hysteresis current controller to control the injected current to the grid. The second controller consists of regular sample PWM controller to control the voltage terminal. The trip signal from the islanding detection algorithm selects which controller will be in service according to the main grid status. To evaluate the performance of the proposed synchronization mechanism and converter controller a simulation model for the microgrid consists of a fuel cell emulator, three phase inverter, wind turbine emulator and local AC loads, as shown in Figure 8.12. The microgrid model was tested under various grid conditions with proposed ASRF-PLL and reconfigurable controller techniques and with the conventional SRF-PLL synchronization technique for comparison.

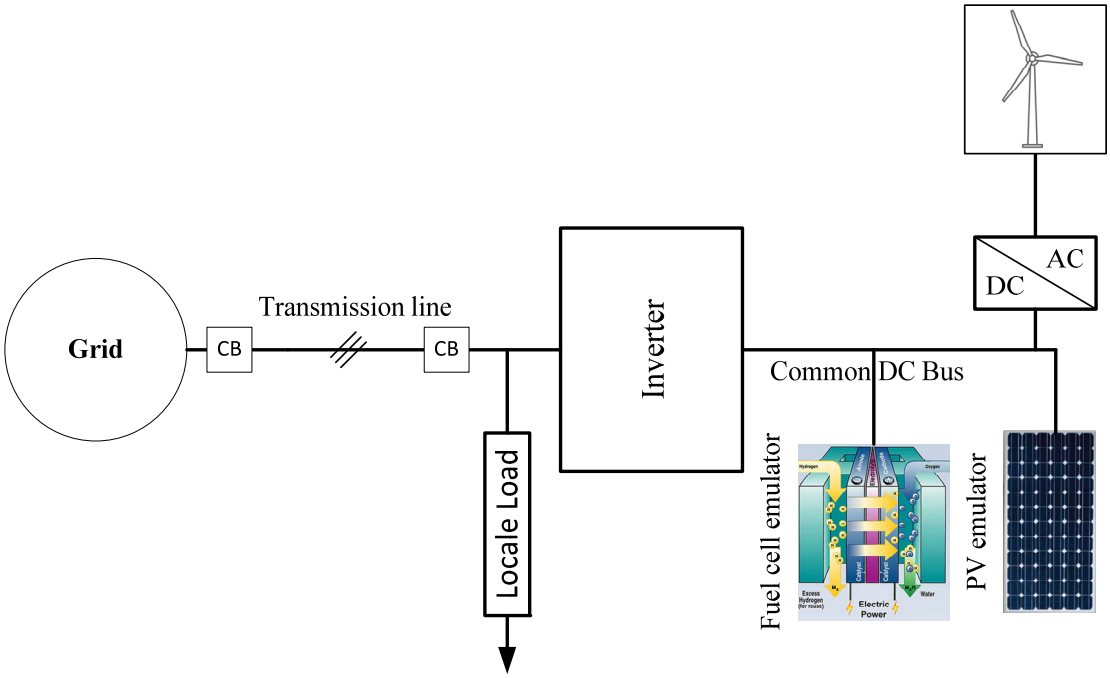


Figure 8.12: Microgrid Block diagram

8.6 Simulation results

The simulation results for the microgrid control with conventional SRF-PLL are shown in Figure 8.13. It is clear that the SRF-PLL produce large frequency oscillation in presence of voltage harmonics. This frequency oscillation increases significantly in the presence of unbalanced voltage at time equal 0.15 second. Moreover, the SRF-PLL completely fails to maintain constant frequency after the grid disconnection at time equal 0.2 seconds. Figure 8.14 shows the simulation results for the proposed ASRF-PLL technique. The simulation results show that the proposed PLL has excellent performance under distorted and unbalanced voltage; it also maintains a constant frequency and accurate phase angle detection under various conditions. This leads to reduction of the current total harmonics distortion from 7.04% with SRF-PLL to 3.22% with the proposed ASRF-PLL. On the other hand, the islanding detection mechanism detects the grid disconnection. The PLL automatically switched to an internal reference, maintaining constant output frequency. The inverter controller successfully changed to voltage control mode and regulates the output voltage.

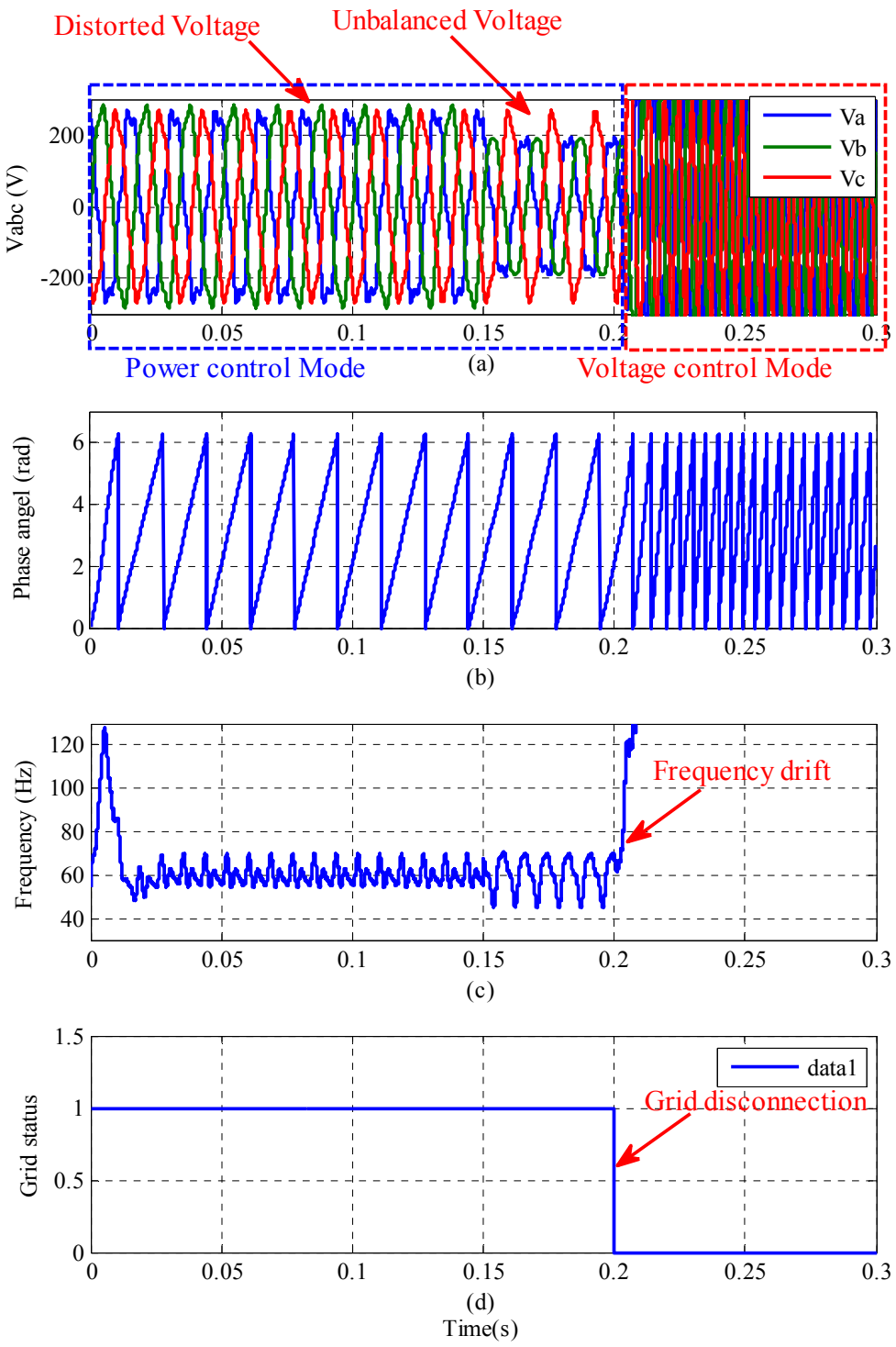


Figure 8.13: Microgrid performance with conventional SRF-PLL. (a) three phase voltage. (b) Estimated phase angle. (c) Estimated frequency. (d) Grid status

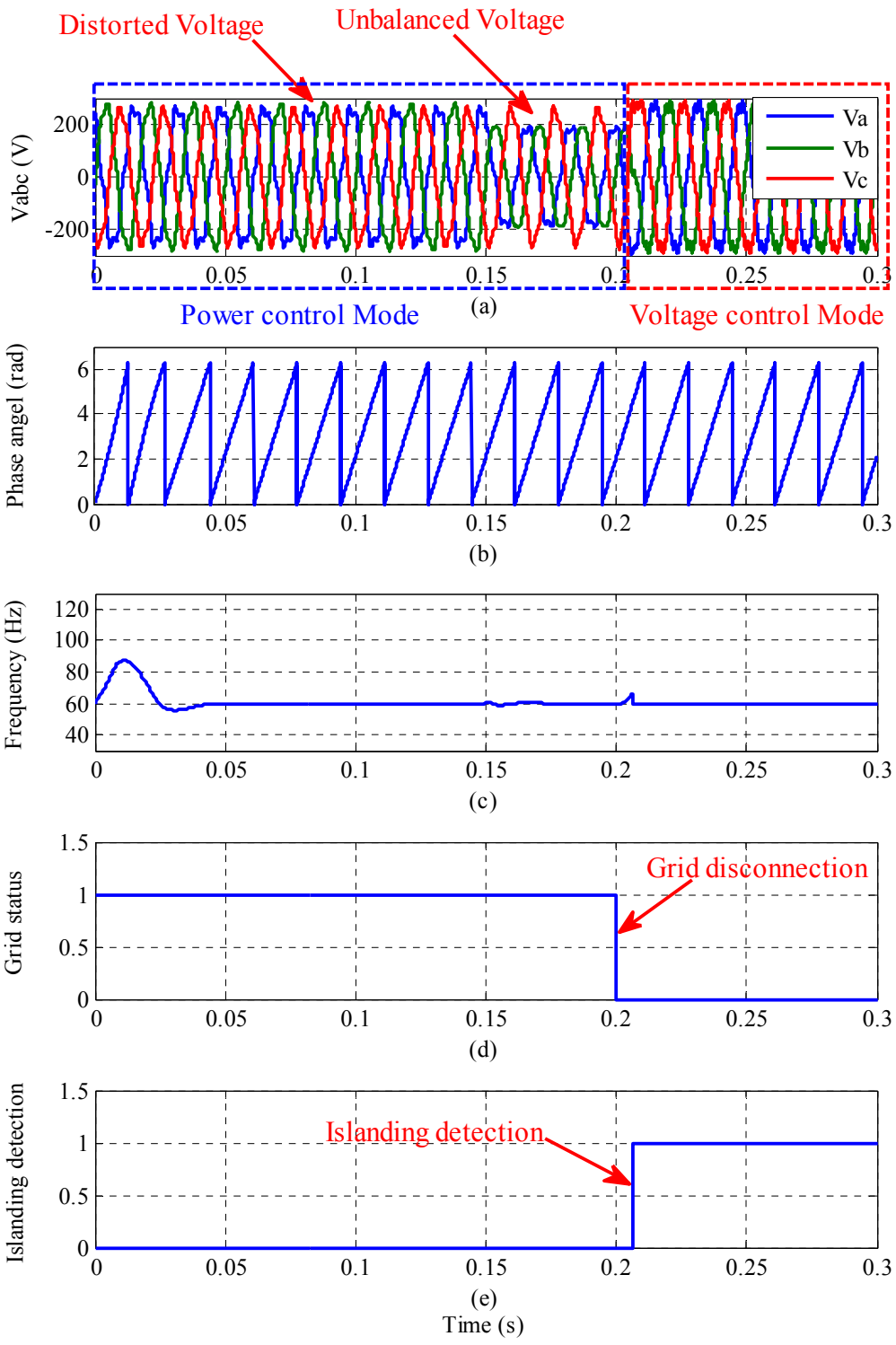


Figure 8.14: Microgrid performance with ASRF-PLL. (a) three phase voltage. (b) Estimated phase angle. (c) Estimated frequency. (d) Grid status

8.7 Experimental results

The proposed ASRF-PLL and reconfigurable inverter controller were implemented using real-time digital controller dSPACE 1103. The experimental test bed shown in Figure 8.15 consists of a 6 kW fuel cell emulator, wind turbine emulator, three phase inverter and an AC grid consisting of four generators.

The experimental result for the SRF-PLL is shown in Figure 8.16. The SRF-PLL has large phase error in presence of voltage distortion and the output frequency is oscillating around 60Hz. Figure 8.17 shows the frequency response for the proposed ASRF-PLL. The results show that the proposed ASRF-PLL performance is excellent under distorted voltage conditions. The phase angle tracking is accurate and the estimated frequency is stable. The islanding detection performance and control reconfiguration are depicted in Figure 8.18. An islanding situation occurs at a time equal to 0.5 Sec. The islanding detection algorithm detects the frequency drift and switches to internal frequency reference. The trip signal initiates control reconfiguration from power control to voltage control mode, which results in stable voltage and frequency.

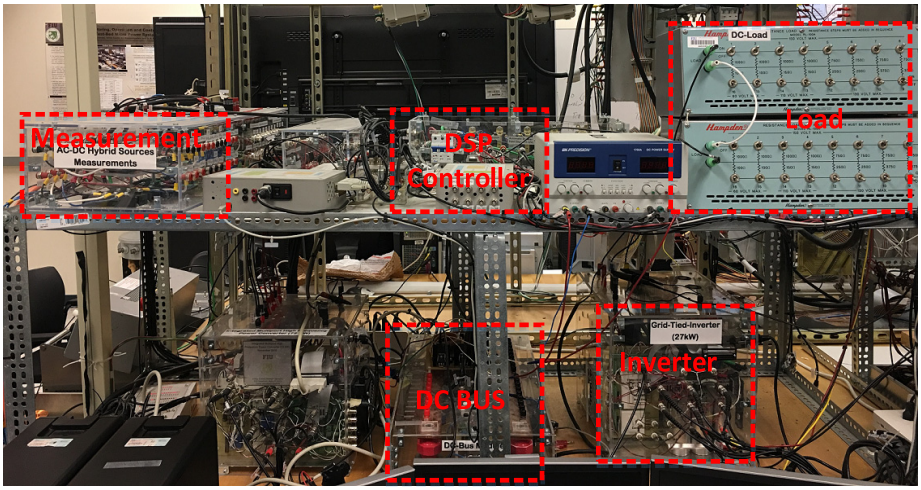


Figure 8.15: Microgrid test bed.

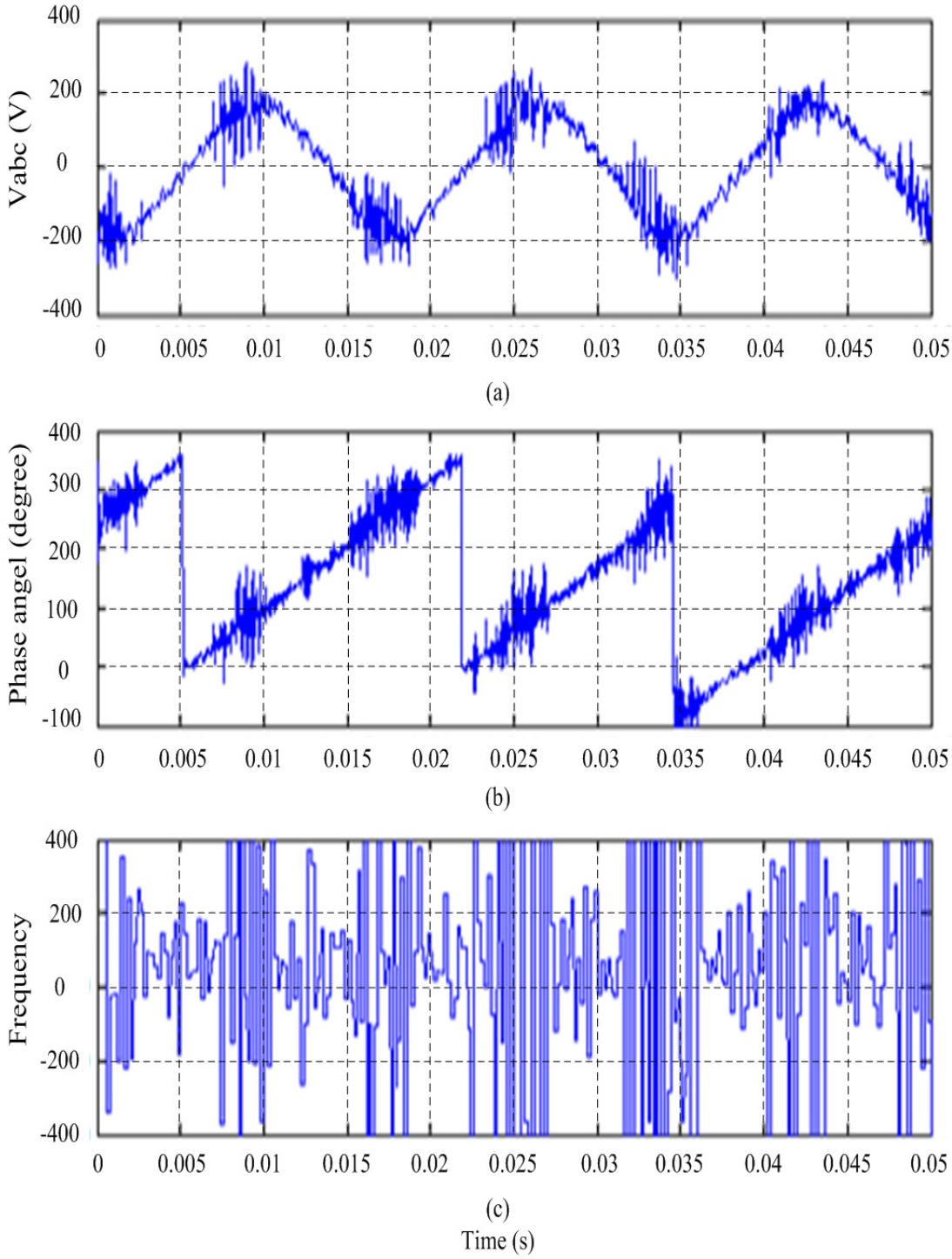


Figure 8.16: Conventional SRF-PLL experimental results. (a) phase voltage, (b) Phase angle, (c) frequency

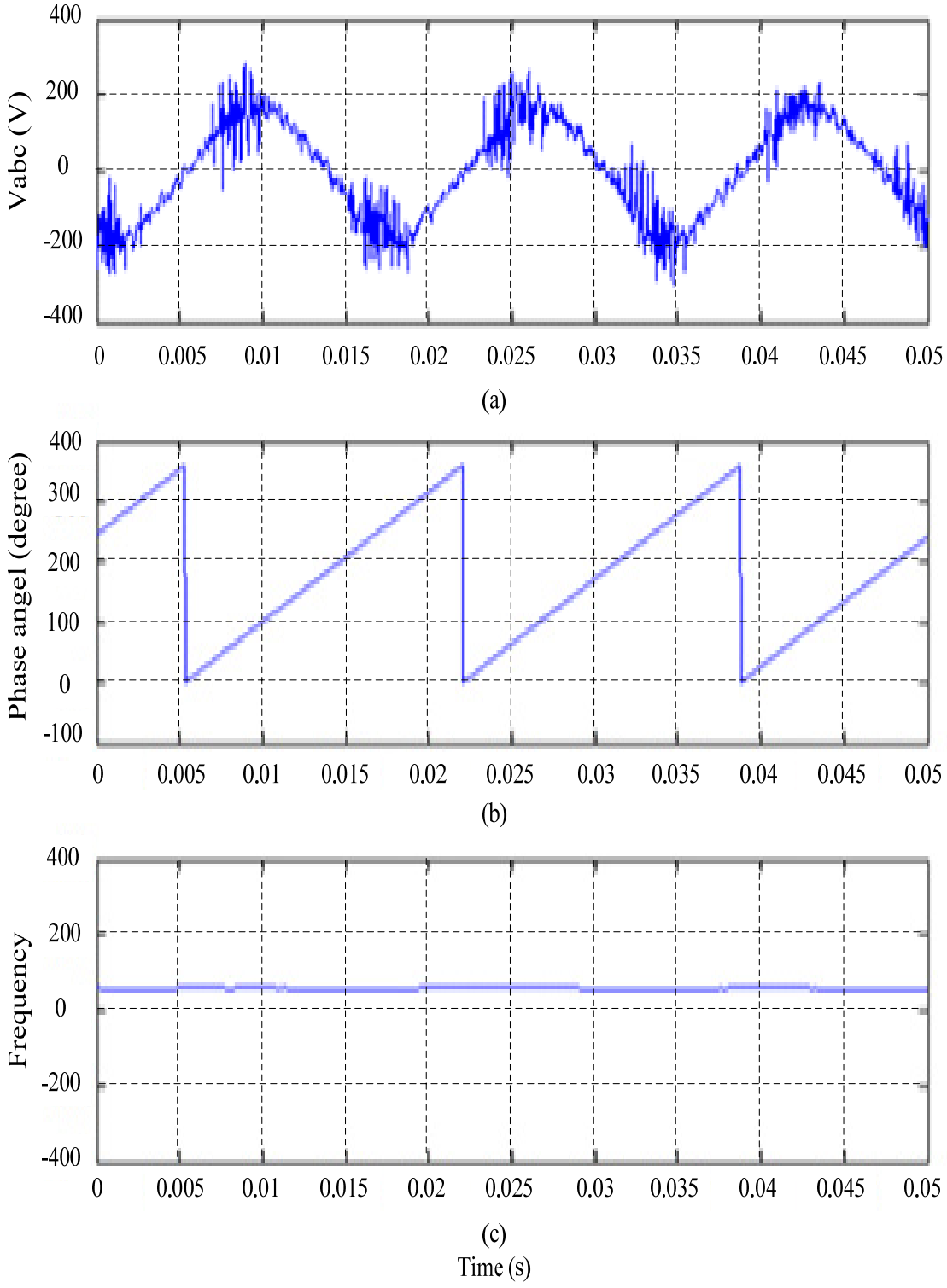


Figure 8.17: Proposed ASRF-PLL experimental results

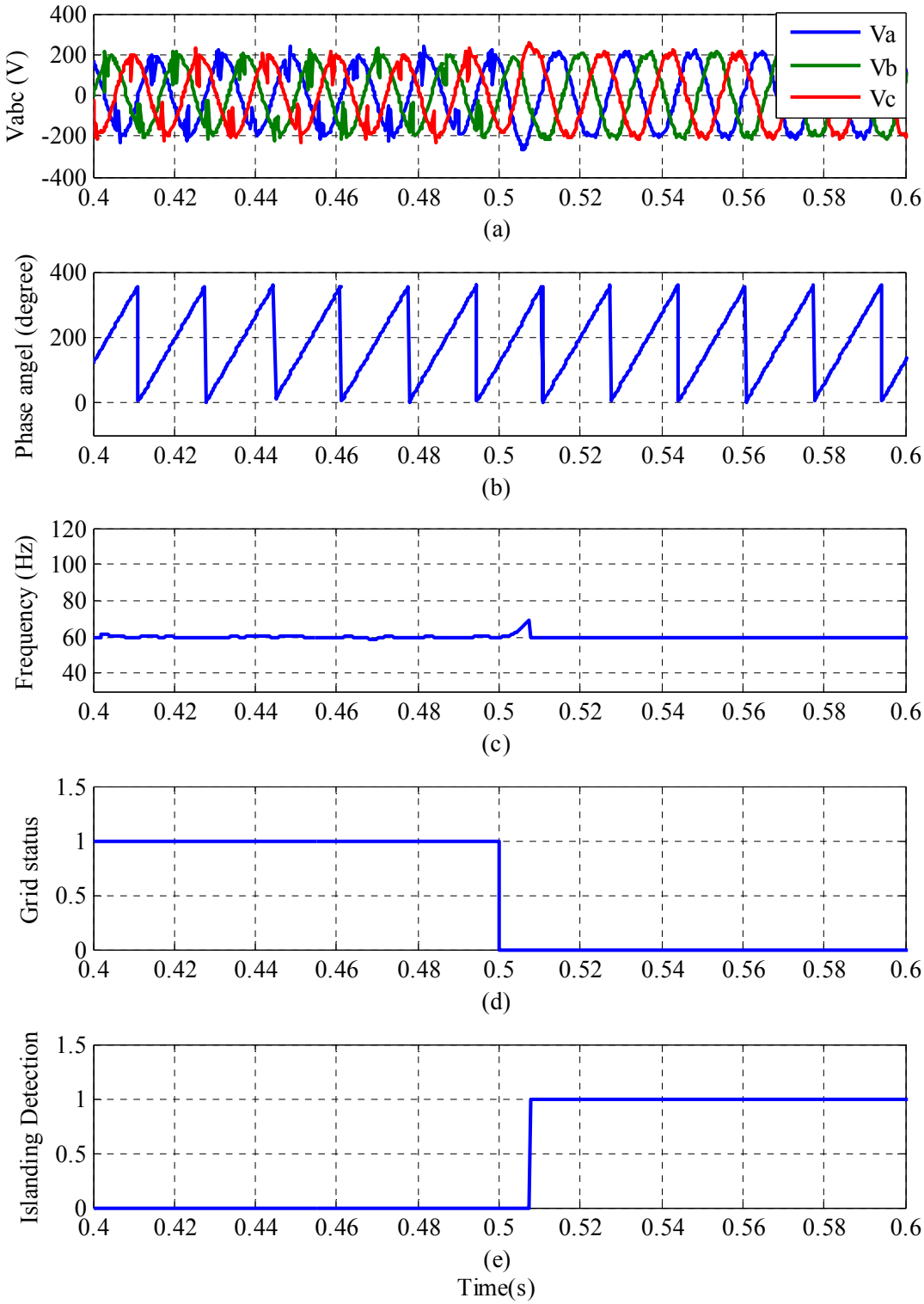


Figure 8.18: ASRF-PLL islanding detection

8.8 Summary

In this chapter, an improved adaptive synchronous reference frame phase locked loop ASRF-PLL with islanding detection is introduced. The proposed technique shows an excellent performance under unbalanced and distorted voltage conditions. In the islanding mode, the detection algorithm succeeds to detect grid disconnection and switch to internal frequency reference. A reconfigurable inverter control is also proposed to maintain stable operation in the grid connection and stand-alone operation modes. The proposed method ensures islanding detection and stable operation of the microgrid when remote islanding detection and SCADA system fails. Both simulation and experimental results prove that the proposed techniques improved the microgrid's performance and stability, and reduce the chance of microgrid service interruption.

Chapter 9 Microgrid Energy Management System

9.1 Introduction

The smart grid is seen as a power system with real-time communication and control capabilities between the consumer and the utility. This modern power system model allows facilities to adopt new technologies and consumers to perceive new services. Utilizing communication technologies, the smart grid topology allows optimization of energy usage based on several factors including environmental, price preferences, and system technical issues. Therefore, the smart grid will be integrated with a smart infrastructure such as smart meters and intelligent controllable devices with advanced two-way communication channels. The latter will facilitate the adoption of distributed EMS [92],[93]. The concept behind energy management is to utilize this two-way communication technology in order to achieve more resilient and sustainable power grids by properly adjusting the power flow from and to the main grid based on present and forecasted pricing, generations, and load information. This is to meet certain operational objectives such as cost minimization [93],[94]. The EMS enables energy consumers to change their consumption patterns by providing them with incentives in a strategy referred to as real-time pricing where utilities vary the energy price in accordance to real-time generation cost [95]. Consumers' bills are thus reduced while achieving flat demand peaks [96].

There have been significant efforts in recent literature on EMS dealing with different points of view and utilizing different modeling and implementation techniques. In the energy trade decision-making processes, most developed EMS models rely on data from

current and forecasted observations. One of the main contributions of this work is the utilization of history, present, and forecasted future data to design an EMS with fine-tuned energy trade decisions. That is, the developed EMS controller makes its decision based on current and forecasted observations, while its parameters are being adapted and optimized by running exploration simulation scenarios based on highly correlated short-term history data. The work presented in this chapter develops a complete EMS framework for small microgrids or nanogrids, which is practical and scalable. The EMS represents the application layer on the top of previously developed physical, communication and control layers. The EMS application will collect information from AMI, sensor network and control power electronics converters, energy storage and distributed renewable energy source to optimize the energy usage and reduce the cost.

As the expertise and manpower present in large utility systems is not always available for operating small microgrids, the communication requirements for EMS in small microgrids are more stringent. Such EMS must be designed for ease of installation, support, and maintenance. This requires a robust, resilient, and distributed communication infrastructure with failover mechanisms. Therefore, the DDS infrastructure is utilized as the communication backbone for all involved entities in the developed EMS as shown in Figure 9.1. Some of the recent work in the literature proposed the utilization of IEC 61850 as the communication framework for EMS for interoperability purposes. However, such implementation utilizes MMS protocol for high-level control applications, GOOSE protocol for event triggered signals, SMV protocol for sensor measurements. The drawback of this is that MMS messages are based

on client-server communications making the EMS not fully distributed. The GOOSE and SMV messages, on the other hand, are non-routable and have a lot of security issues because they are unencrypted broadcast messages. More details on IEC 61850 security will be discussed in chapter xx. It is noteworthy to mention that the DDS middleware is expandable and provides a standard API, which allows its integration with different systems. This allows mapping standard data models such as IEC 61850 into DDS.

The developed EMS was tested on load consumption data for residential areas and solar energy patterns in Miami, Florida, USA for the year 2014 [97] applied on emulated microgrids models on hybrid hardware/software simulation environment. The developed control modules were built in SIMULINK simulation environment, converted into a C code and were run in real time. To account for practical networking issues, software modules were integrated with a DDS communication middleware to exchange the data over a real Ethernet network [98]. Additionally, an appropriate QoS profile was set for each application as will be explained later. The hybrid modeling environment allows accurate emulation of the proposed EMS as an integrated cyber-physical system. Real-time pricing and time-of-use price schemes were adopted in different case studies for months in winter and summer seasons. The results showed that the developed EMS was successful in providing significant savings in the microgrids power consumption cost and, in some cases, achieved profit.

9.2 Real-time communication infrastructure for microgrid control

Microgrid distributed control requires data exchange between different components and applications for efficient energy management and economic operation.

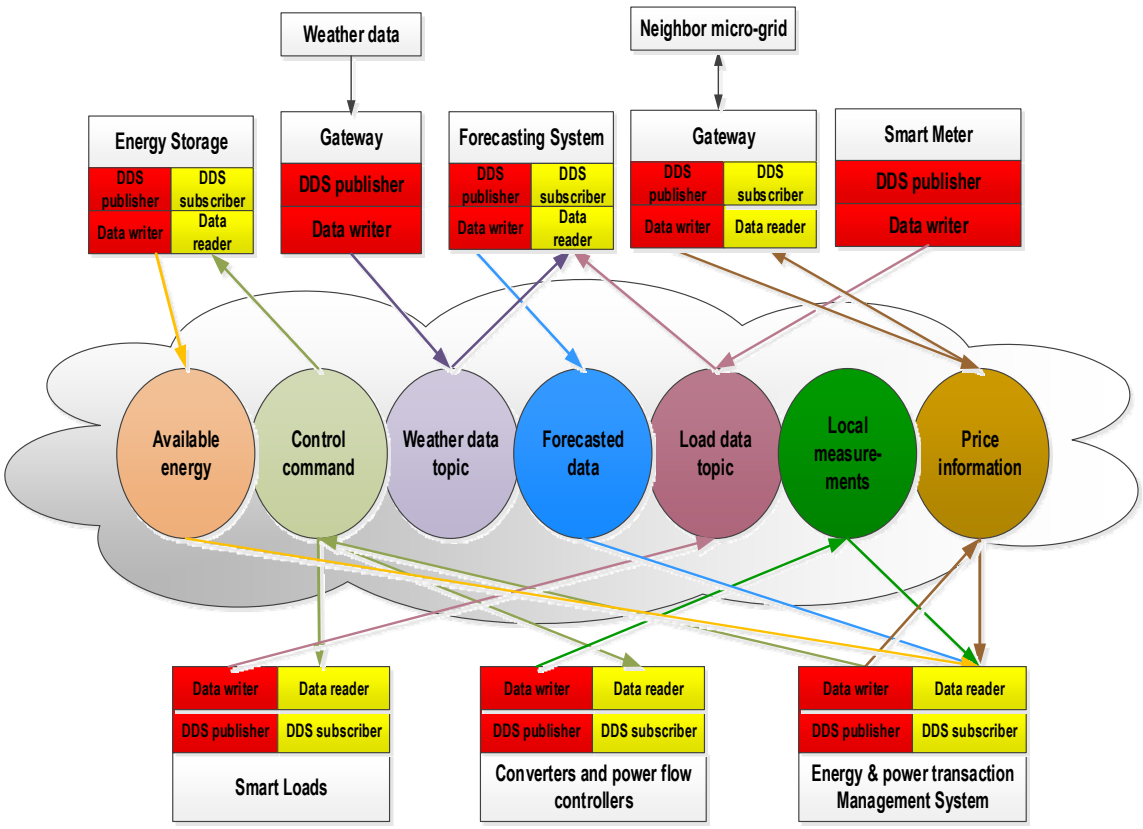


Figure 9.1: Proposed DDS Network and Microgrid Logical Control Hierarchy

For instance, during its decision-making process, an energy management control system requires information exchange with smart meters, energy forecasting systems, energy storage, and other entities to decide on an appropriate energy transaction. Also, a demand side management application needs to exchange information pertaining load priorities and price information to send appropriate control commands to smart loads. Embedded controllers for power electronics converters, which manage the direction and amount of power flow, need to receive real-time control commands and send feedback signals to the control system as well. Moreover, the balancing between loads and generation in small microgrids with variable renewable energy sources and/or low inertia generators relies on fast communication and data exchange to maintain the overall system

stability. Each of the aforementioned applications and components has different communication requirements and require different security levels. The data and events were exchanged among different EMS modules using the developed DDS network utilizing peer-peer communication scheme. Figure 9.1 shows the proposed DDS network structure and the logical relations between various publishers and subscribers. In this chapter, the communication requirements for each type of application and component was analyzed to determine the updating data rate and quality of service required for each one. Redundancy paths and failover mechanisms to ensure operation continuity under communication failure or cyber-attack incidents were also studied.

9.3 Intelligent microgrid control

The intelligent control of the microgrid relies on seamless integration between multiple modules, such as load forecaster, energy management controller, renewable energy controller, energy storage and AMI. These modules will be discussed in detail in the following sections.

9.3.1 Energy management system

The system under study in this work is composed of an electric power utility and a scalable set of N microgrids as shown in Figure 9.2. Each microgrid has its own renewable energy generation resources, energy storage devices, and local loads. At all times, it is assumed that the microgrids are operating in grid-connected mode via a bidirectional grid-tied inverter. Two scenarios arise here: the first is when the microgrid has excess energy and needs to sell power to the utility, and the second is when the microgrid has deficient energy and needs to buy power from the utility. As can be seen in

Figure 9.2, the migration between the two modes of operation is decided upon by the control signal, Direction of Power Flow, coming into the grid-tied inverter. Moreover, not only does the controller decide on the direction of the power flow, but also it decides on the percentage of the power to be sold to or bought from the grid. That is, in the excess energy case, and after covering the microgrid's local load, the controller outputs a power reference signal, which dictates what percentage of excess energy is to be stored in local energy storage devices and what percentage is to be sold to the utility. Contrary to this, in the energy deficiency case, the controller checks how much power is needed to cover the local load and purchases that amount from the utility. The controller presented is based on a set of fuzzy logic rules and takes its decision based on several input parameters which will be detailed in the section 9.3.3.

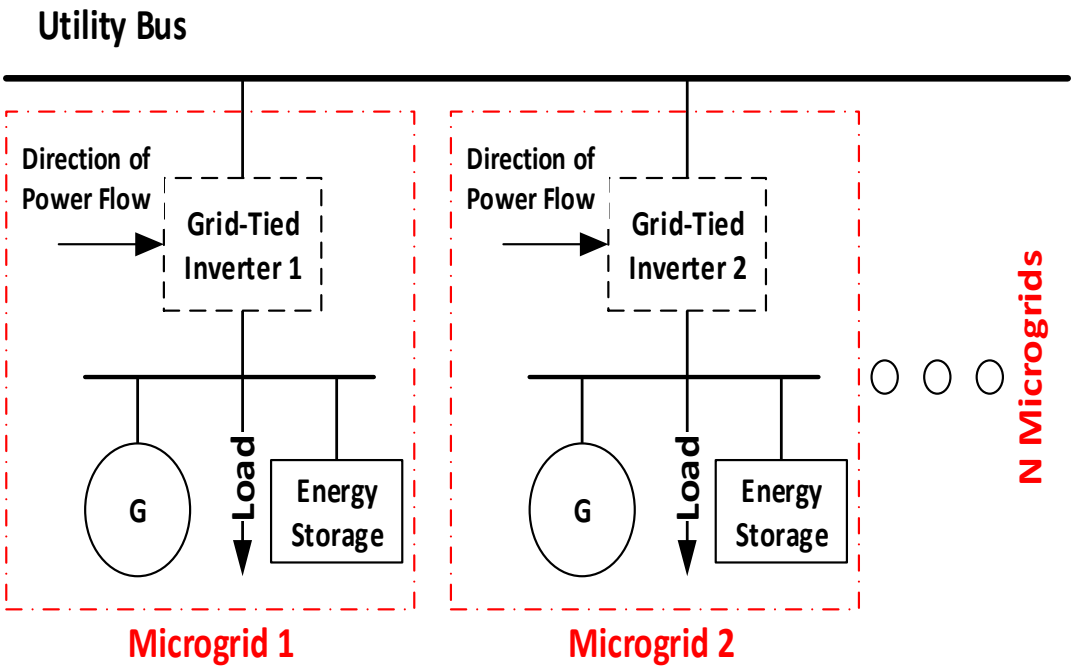


Figure 9.2: Overall System Topology

9.3.2 Advanced Metering Infrastructure and Energy Pricing Mechanism

Advanced Metering Infrastructure allows bi-directional information exchange between smart meters and utility control centers. Smart meters send consumption information usually on an hourly basis and receive price information and control commands from the smart meter head-end. The main target of an AMI implementation is to allow demand side management and cost management [99]. To achieve this goal the AMI standard allows exchanging information between smart meters and customer devices and systems through the customer gateway. The smart meter sends small data packets for basic power consumption information [99]. The transmission rate of the formal could be defined per minute or per hour depending on the application need. Usually, the sensitivity of smart meter information exchange to communication delays inside a microgrid control network is relatively low; however smart meter data requires a high level of availability. Some applications utilizing smart meter data such as load and price forecasting depends on current and previous data to be persistent. Data persistence can affect the performance of such applications, especially in the case of losing and restoring communication. From a cyber-security point of view, smart meter data needs a high level of confidentiality to ensure customer privacy and data authentication to prevent replay and false data injection attacks. To secure the smart meter data on the GDS, DDS persistence and encryption features can be used to protect the data confidentiality and maintain last transmitted samples for newly joined devices.

Two pricing mechanisms were adopted in our case studies. The first is a real-time pricing scheme, whereas the second is a time-of-use (TOU) pricing scheme. For real-time pricing, the energy management system will receive hourly pricing via AMI.

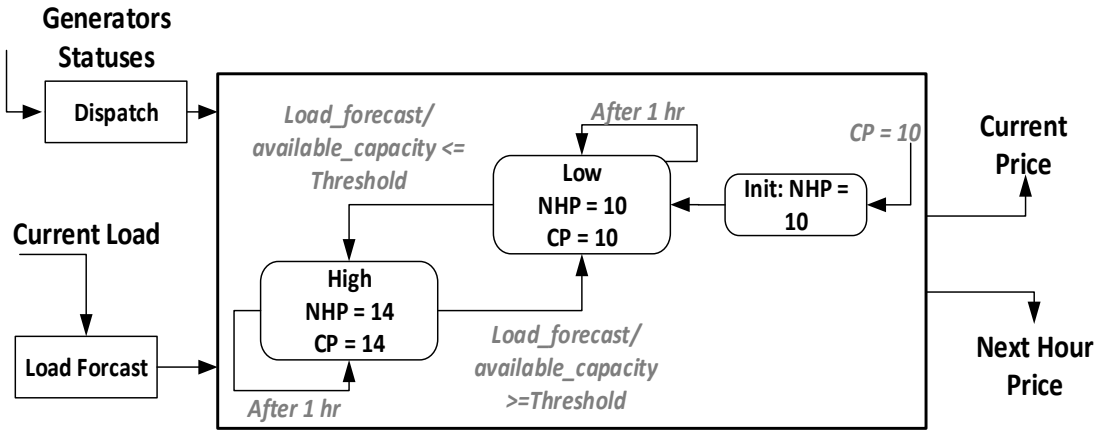


Figure 9.3: Real-Time Pricing Algorithm

The utility company will change the energy price based on forecasted load and generation status. The utility controller takes generators statuses and total forecasted load as inputs and outputs the current and next hour energy price (CP and NHP respectively). The price of electricity is decided upon on hourly basis by a state flow control logic shown in Figure 9.3 and is divided into two categories: Low (10 cents/Kwh) and High (14 cents/Kwh). Here, a gateway is utilized to exchange pricing information between the energy management system and the smart meters. This gateway receives the real-time pricing from smart meters over a ZigBee wireless link and publishes it using publisher/subscriber protocol. The published price is available on the Global Data Space (GDS) for all interested applications such as the EMS and forecasting modules shown in Figure 9.1. Since the price signal has a low update rate, a persistence QoS feature has been enabled for it. This QoS ensures delivery of the last price to newly joined devices without periodically retransmitting the data. To prevent fake data injection attack on the price signal, which impacts the customer consumption cost, Price signal can be authenticated with the digital signature algorithm. For the time-of-use pricing scheme, a

predefined price schedule is set for on-peak and off-peak energy consumption hours. The adopted profile is that set by Florida Power and Light Company (FPL) with two sets of prices. One for on-peak hours with a positive rate of 9.154 c/Kwh and another for off-peak hours with a negative price rate of -4.072 c/Kwh [100]. For this pricing scheme, no communication is required since the pricing profile is predefined for a long period of time.

9.3.3 EMS Fuzzy Logic Controller

The microgrid controller is a fuzzy controller based on the Sugeno-like model. The controller takes the batteries state-of-charge (SOC), current price (CP), next hour price (NHP), available energy (AE) and forecasted local load demand (FLD) as inputs and produces the microgrid's reference power (P_{ref}) as output as shown in equation (9.1).

$$P_{ref} = f(SOC, CP, NHP, FLD, AE) \tag{9.1}$$

By this method, the fuzzy logic controller decision is based on current and future observations of the microgrid state. The decision of the fuzzy controller is based on a rule surface composed of a set of 90 logic rules. Each of the five inputs (SOC, CP, NHP, AE, and FLD) are passed through trapezoidal membership functions spanning the complete range of their corresponding inputs. The firing strength of each rule is then evaluated and a crisp value of the output is calculated using the weighted average defuzzification method.

The controller output is used to control the direction and amount of power flow through the grid-tied inverter. Therefore, the charge control signal for the energy storage devices, CC, is defined in equation (9.2) as:

$$CC = AE - P_{ref} \tag{9.2}$$

This means that the battery will be charging either from the renewable energy sources in the case of $AE > P_{ref}$ or from the utility when $P_{ref} < 0$ indicating a reverse power flow from the AC side to the DC side on the grid-tied inverter. The SOC of the energy storage devices depends on the total amount of energy transferred to the storage devices minus the losses due to devices' efficiency as in equations (9.3) and (9.4).

$$SOC(t) = \frac{W_{ES}(t)}{ESC} \times 100 \tag{9.3}$$

$$W_{ES}(t) = W_{ES}(t-1) + CC(\Delta t)\eta \tag{9.4}$$

Where W_{ES} is the total energy stored is, ESC is energy storage capacity, and η is the energy storage efficiency. The net power sold to or purchased from the utility is expressed in equation (9.5) as:

$$P_{utility} = LLD - P_{ref} \tag{9.5}$$

Where a positive $P_{utility}$ indicates purchasing energy from the utility, while a negative $P_{utility}$ indicates selling energy back to the utility. The energy transaction logic is shown in Figure 9.4.

9.3.4 Forecasting

A feed forward neural network trained using the Levenberg – Marquardt back propagation algorithm was used in order to forecast the hourly load demand and the anticipated power generated from the renewable energy sources in the microgrid. In most applications, neural networks are trained offline using bulk data sets to obtain a fixed set

of weights and biases, which are used afterward over the entire forecasting horizon. This strategy will be fine if applied to a simple problem or if the forecasting is done over a small-time scale.

However, in the case of individual load demands for small microgrids, especially in the era of information security, a large amount of customer data for training could put customers' privacy at risk if disclosed. For that, this work used an adaptive training technique entailing online update of the neural network's weights and biases over short time periods. The neural network receives information about current load demand, previous hour load, weekday, day number, time and the day type (Normal day or holiday) and forecasts the next hour's demand. In the adopted online training technique, the load of each next hour is compared with its forecasted value and the error is back propagated to fine tune the weights and biases as mentioned earlier. The load forecasting module receives data from the GDS shown in Figure 9.1. Since the forecasting algorithm depends on current and previous data samples, communication loss could impact the forecasting performance drastically. The DDS QoS could minimize the impact of communication loss on the forecasting algorithm by keeping N history samples. These samples will be delivered instantly to the corresponding subscribers upon communication restoration. Figure 9.5, shows the performance of the forecasting module upon losing samples 12 and 13. In **Error! Reference source not found.** (a), a historical length (N = 2) is defined, whereas in **Error! Reference source not found.** (a) and (b) this QoS feature was not activated. As can be appreciated from the figure, the forecasting module was immediately able to catch up after the communication was restored, while in case of

Error! Reference source not found.(b), it took the forecasting module 2 samples to catch up.

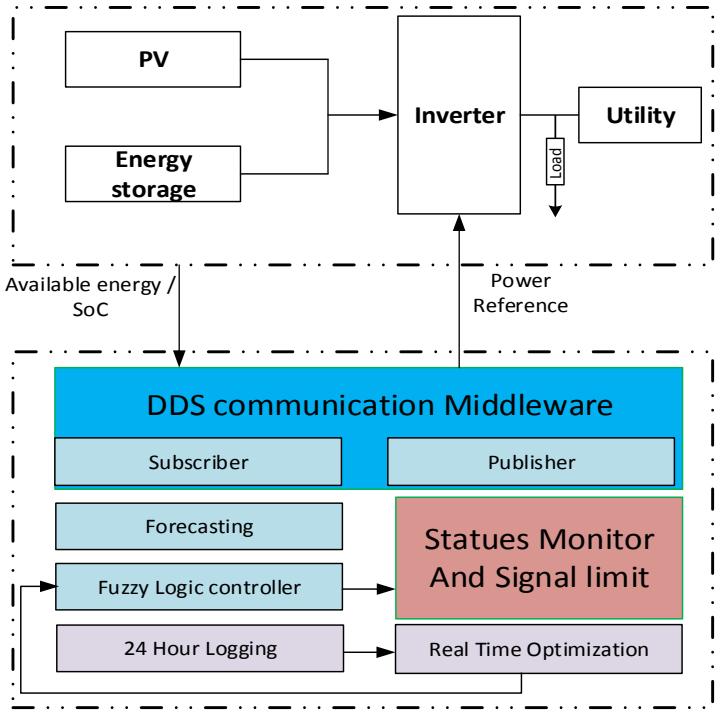


Figure 9.4: Energy Transactions Logic

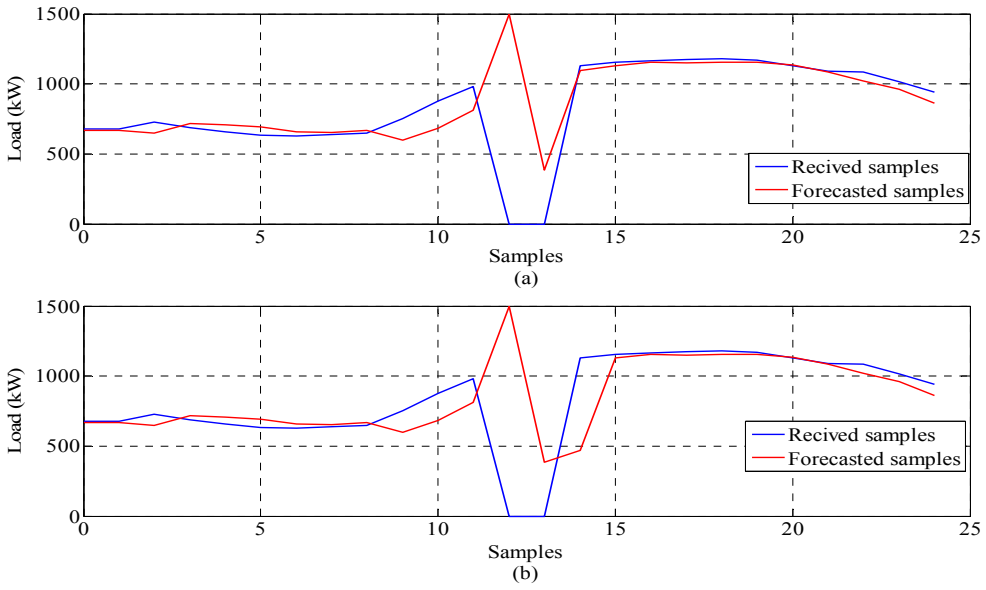


Figure 9.5: Performance of neural network (a) with persistence QoS (b) without persistence QoS

9.4 Real Time Online Optimization of Controller Parameters

As discussed earlier, the purpose of the energy management system is shifting peak loads of individual microgrids from high energy price periods to lower energy price periods. In order to ensure minimal expenditure and maximal profit for the microgrid, an online parameter optimization scheme based on Particle swarm optimization (PSO) for the fuzzy logic controller parameters was developed.

The optimization process proposed in this work is periodic with a period of 1 day. That is, at the beginning of each day, the collected data are fed into the optimizer and the optimization process is initiated to come up with new optimized controller parameters for that day. Figure 9.6 shows the chronological order of the optimization process. It can be seen that the optimization process requires some time to finish and this depends on the adopted processor's speed. In this study, the maximum optimization time recorded was 23 mins on an Intel core i7 processor (3.50 GHz). This time could be further reduced by implementing parallel processing utilizing multiple processor cores simultaneously. It is worth noting that the optimization process in this work falls into the category of exploration simulation. That is, during the second day, while the system is up and running, the optimization process is being executed in the background on a simulated microgrid model to explore the performance of the new optimized parameters. Once the process is finalized, the controller's parameters are updated online without any disturbance to the overall system operation. Consider the three-day period shown in Figure 9.6. During the past 24 hrs, measurement units in the microgrid are continuously

collecting data about available energy, local load demand, current price, next hour price, and state-of-charge of the microgrid's energy storage devices.

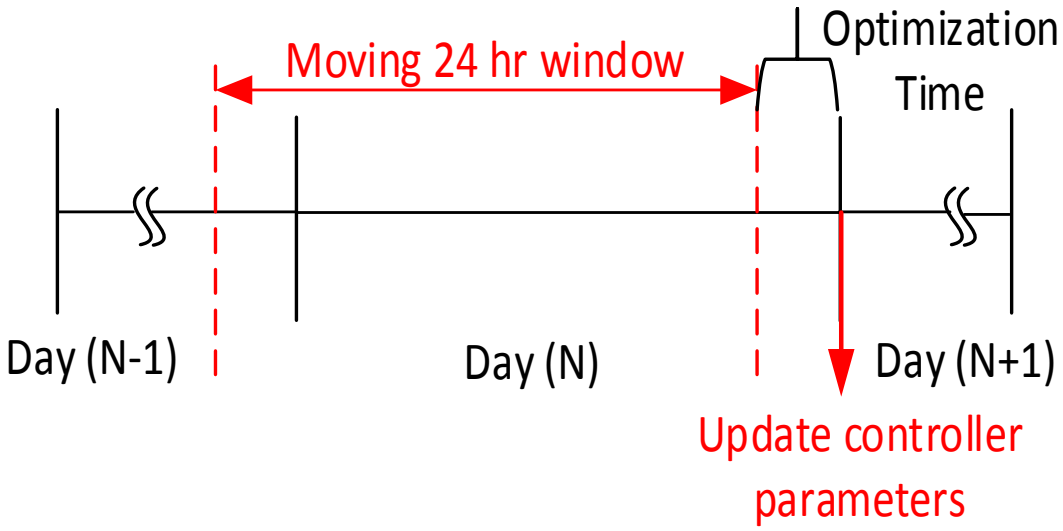


Figure 9.6: Optimization Process

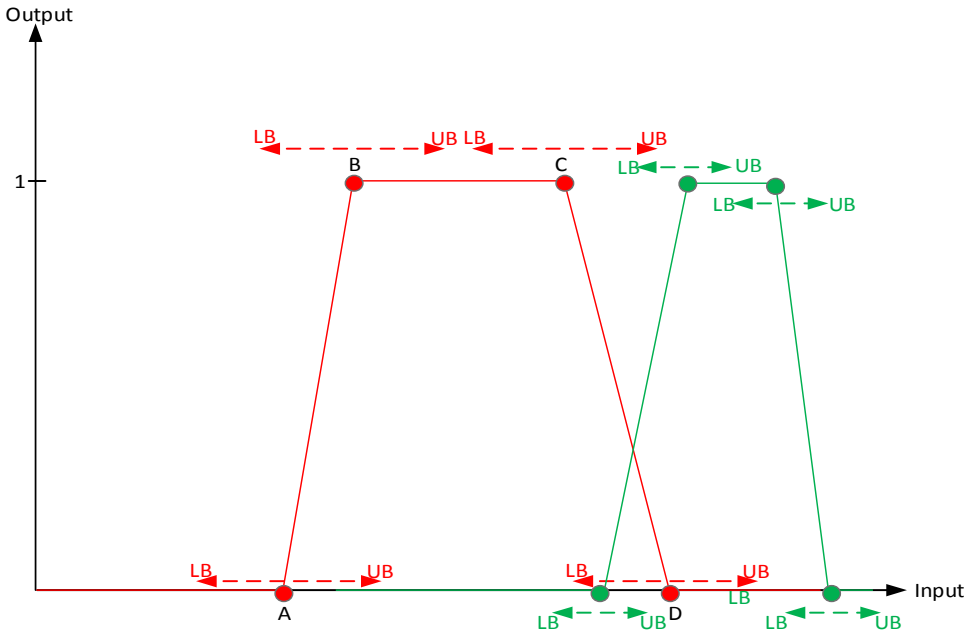


Figure 9.7: Constrained Search Space for Trapezoidal Membership Functions

All collected data for the past 24 hrs window are stored in a temporary database. At the end of the first day, the optimization process initiates. First, a search space is

randomly generated by defining a population of varying combinations of membership functions. The population generation process is bounded by a vector of lower bounds (LB) and upper bounds (UB) for each of the vertices of the membership functions. The Proper definition of the lower and upper bounds is critical for the success of the optimization process Figure 9.7, shows the search space for a given trapezoidal membership function. In order to ensure proper operation of the fuzzy controller, the condition that A < B < C < D must be met. Also, assume that red membership function corresponds to a low SOC and the green membership function corresponds to a high SOC. It is important, thus, that the green membership function remains to the right of the red one. All these conditions have been taken into account in the setting of the lower bounds and the upper bounds vectors. The objective function to be minimized is shown in equation (9.6).

$$min\left(\sum_{h=1}^{24} P_{utility}(h) \times Cost(h)\right) \tag{9.6}$$

In a unique exploration simulation approach for fitness function evaluation, a software model of the physical microgrid with its controller was developed and used to simulate the response of the microgrid to the various particles in the swarm and evaluate the profits and expenditures. In all situations, the optimization process is bound by the constraints of checking that the microgrid is covering its base load and that the energy storage devices are maintained at a proper state of charge that does not deteriorate them. For example, lead-acid battery life could be extended significantly if its SOC does not fall below 40% [101]. The optimization process is repeated until the combination of membership functions that results in better utilization of the microgrids energy storage to

shift peak loads to low price periods is achieved. Once the optimum membership functions are obtained and verified in the background simulation, the real time controller is updated with the new functions. Repeated optimization process allows the system to adapt to change on the customer behavior and price pattern.

The microgrids, EMS algorithm, energy storage, renewable energy and load controllers are developed on SIMULINK MATLAB and converted to a C code to run in real time. Instead of having all the modules exchange data internally within the MATLAB environment, the developed modules are integrated with a DDS communication middleware to exchange the data over a real Ethernet network. This approach was adopted in order to account for networking issues such as packet drop, latency, and QoS. An appropriate QoS profile was set for each application as explained earlier. The merging of real network, hardware and simulation software creates a hybrid modeling environment that allows accurate emulation of the proposed EMS as an integrated cyber-physical system. Finally, a software module representing a smart meter head end collects all consumption measurements, feeds the data to the utility pricing module, and publishes back the real-time energy prices.

9.5 Security and failover

It is important to highlight several features in regards to the security of the proposed energy management framework. First, as explained earlier, the proposed EMS is composed of several distributed nodes each serving its purpose. For that, a redundancy scheme has been introduced for each distributed controller. This is achieved by the failover mechanism provided by DDS. Figure 9.8, shows a primary controller (A) and a

redundant controller (B) both having the same feedback and issuing the same control command. However, the owner strength of the primary controller's command is higher. Controller B comes in game when controller A fails.

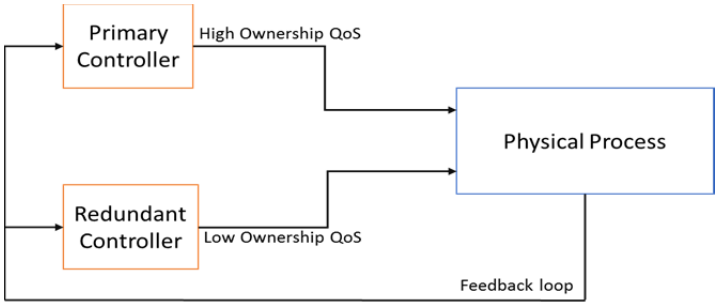


Figure 9.8: Failover Mechanism

Second, along with flattening peak loads, the EMS will ensure the privacy of the customer's data by camouflaging his load demand profile. This is feasible by the utilization of renewable resources along with energy storage devices. This is emphasized in the results in the next section where the shape of the utility power curve is a camouflage of the actual customer load demand curve. Therefore, the customer's behavior is secured and cannot be inferred even if such curves were disclosed.

Finally, all communication are encrypted and all joining nodes are authenticated using DDS Secure.

9.6 Results and Discussion

In this section the results of applying the proposed Energy Management System with and without online optimization on the collected load and solar irradiance measurements from Miami, Florida, USA in winter and summer seasons. The month of January has been selected to represent the winter season, whereas the month of August was selected

to represent the summer season. Additionally, each case was repeated with two pricing profiles as explained before. The first is a real-time pricing scheme, while the other is a TOU scheme with values collected from FPL Company.

9.6.1 EMS performance with real-time pricing scheme

Figure 9.9 and Figure 9.10 show the result of applying the proposed energy management algorithm with real-time pricing scheme, first without using optimized parameters and second with using the daily optimized parameters in the winter season. Looking at the zoomed parts in Figure 9.9, the original load profile had peaks during high energy prices periods. The proposed EMS fuzzy controller without optimization was successful in reducing these peak values by managing the consumption from energy storage and renewable resources. In the winter season, the peak load at time t = 6.8 days, which corresponds to a high price period, was reduced from 3600 W to 2571.3 W. Figure 9.10 emphasizes the importance of the proposed online optimization technique by further reducing the amount of consumed power during high prices to 0 W. This because the optimized EMS has better utilization of the energy storage devices in the microgrid. Looking at the SOC profile, one notices that the SOC with optimization ranges between 60-100%, whereas with optimization it ranges between 40-100%. These results are also asserted in the summer season as shown in Figure 9.11and Figure 9.12 where the peak load at t = 7 days dropped from 3600 W to 2628.3 W without optimization and further reduced to 0 W with optimization. Similarly, the SOC with optimization ranges between 60-100%, whereas with optimization it ranges between 40-100%.

9.6.2 EMS performance with TOU pricing scheme

Figure 9.13 and Figure 9.14 show the result of applying the proposed energy management algorithm with TOU pricing scheme, first without using optimized parameters and second with using the daily optimized parameters in winter season Looking at the zoomed part in the Figure 9.13, during the on-peak period starting from t = 6.75 days to 6.917 days in winter season, the peak consumption was reduced from 2506 W to 1790 W. Here, the customer was still purchasing power from the grid. However, with the optimization algorithm, during this period, the consumer was selling 716.1 W to the utility as shown in Figure 9.14. Again, this is due to an optimum decision of charging and discharging time of energy storage. Figure 9.15 and Figure 9.16 show that during the summer season with TOU pricing scheme, the original EMS controller parameters performed so well that the optimization scheme showed negligible improvements on the overall performance.

Table 9-1 reflects the overall monthly cost of the proposed system for all case studies. For real-time pricing, the overall savings with optimization in the winter and summer seasons was 14.86% and 18.56%, respectively. For the TOU pricing scheme, the total savings were 107.5% and 915.30% for winter and summer seasons, respectively. Percentages higher than 100% means that the customer is making a profit.

Table 9-1: Total Savings

Pricing	Season	Total Cost Without EMS	Total Cost with EMS	Total Cost with Optimized EMS
RTP	Winter	$ 145.74	$ 134.76	$ 124.08
	Summer	$ 90.81	$ 84.12	$ 73.95
TOU	Winter	$ 55.77	$ 17.16	$ -4.2
	Summer	$ 2.94	$ -23.94	$ -23.97

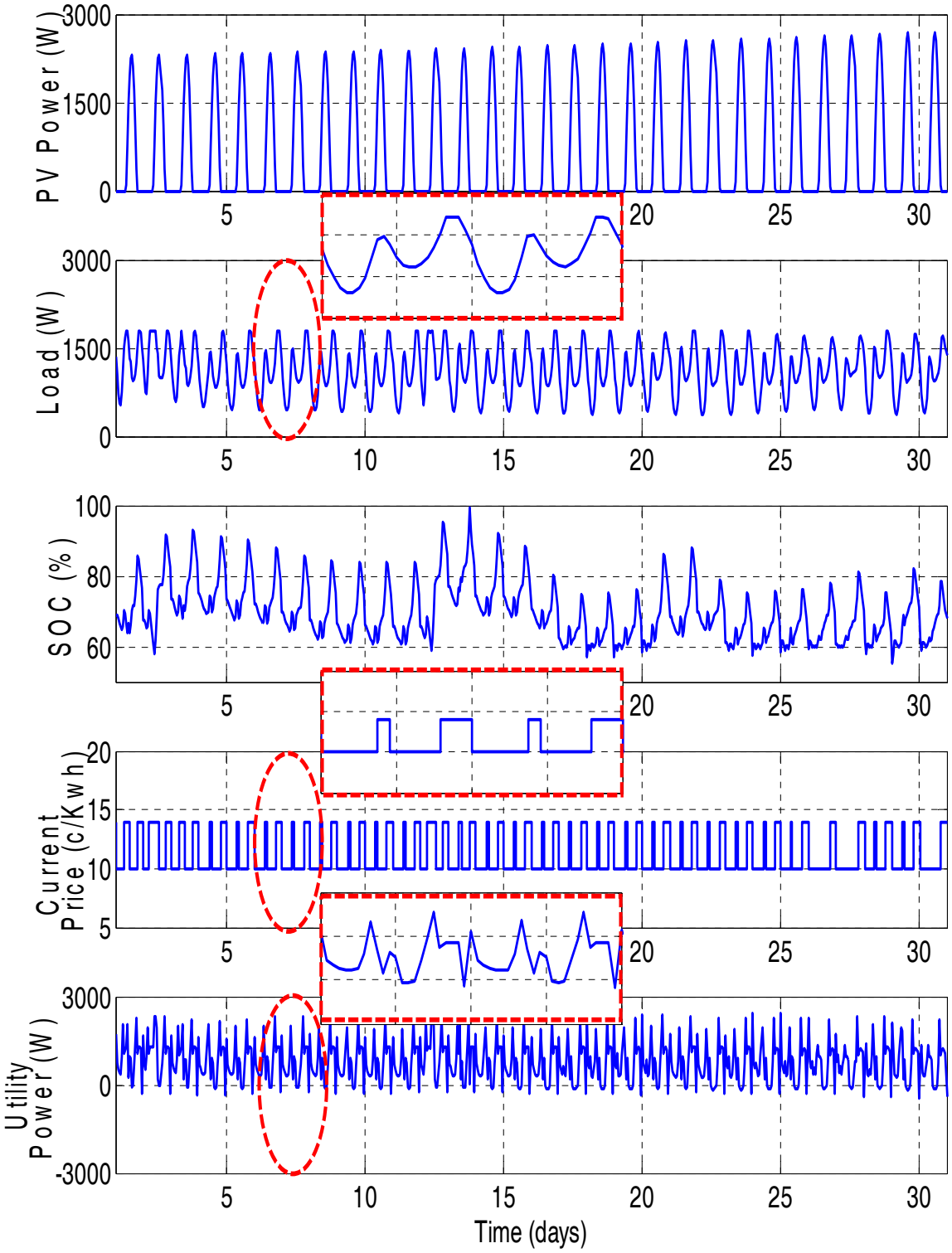


Figure 9.9: Winter Real-time Pricing without Optimized Parameters

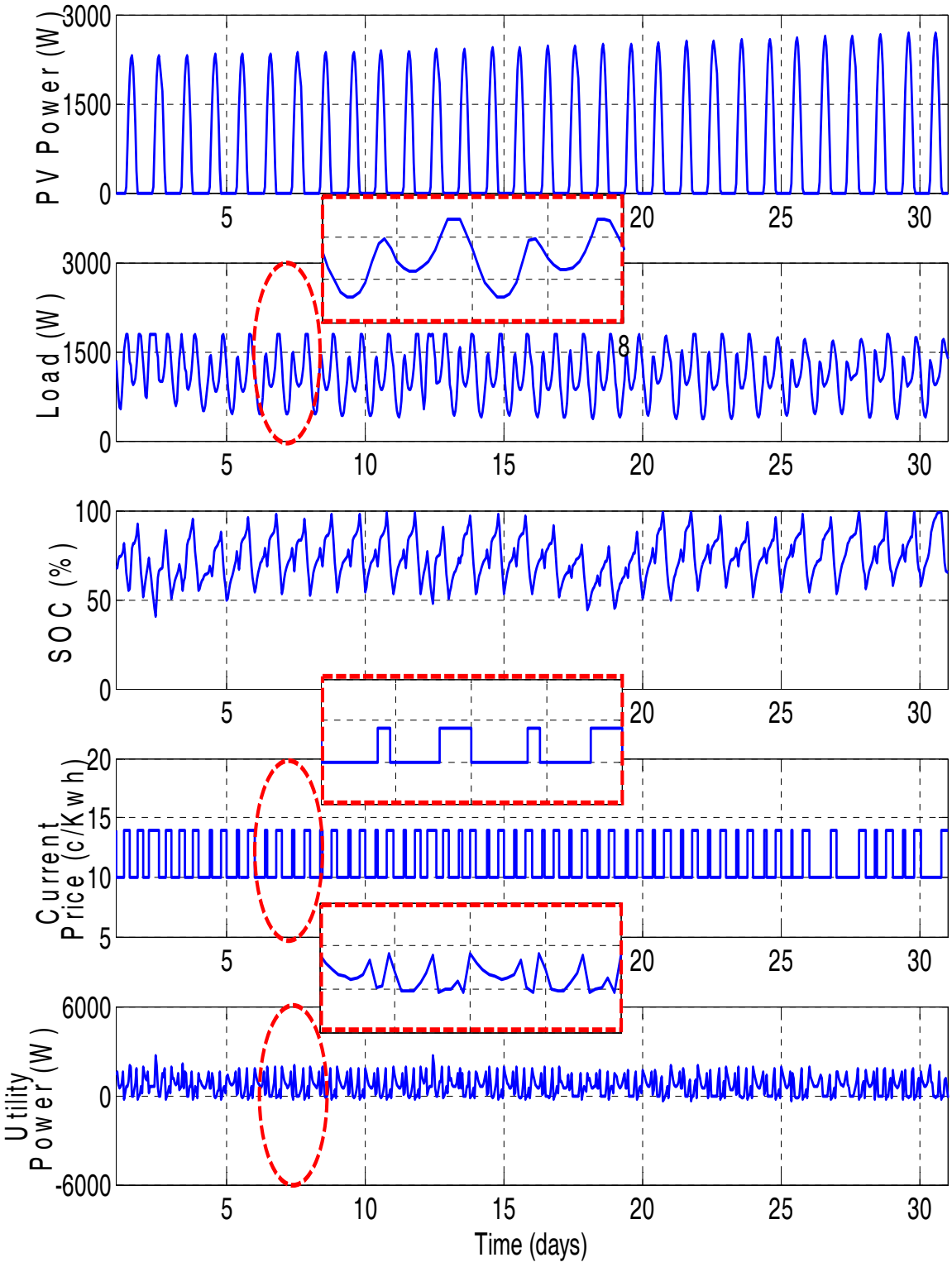


Figure 9.10: Winter Real-time Pricing with Optimized Parameters

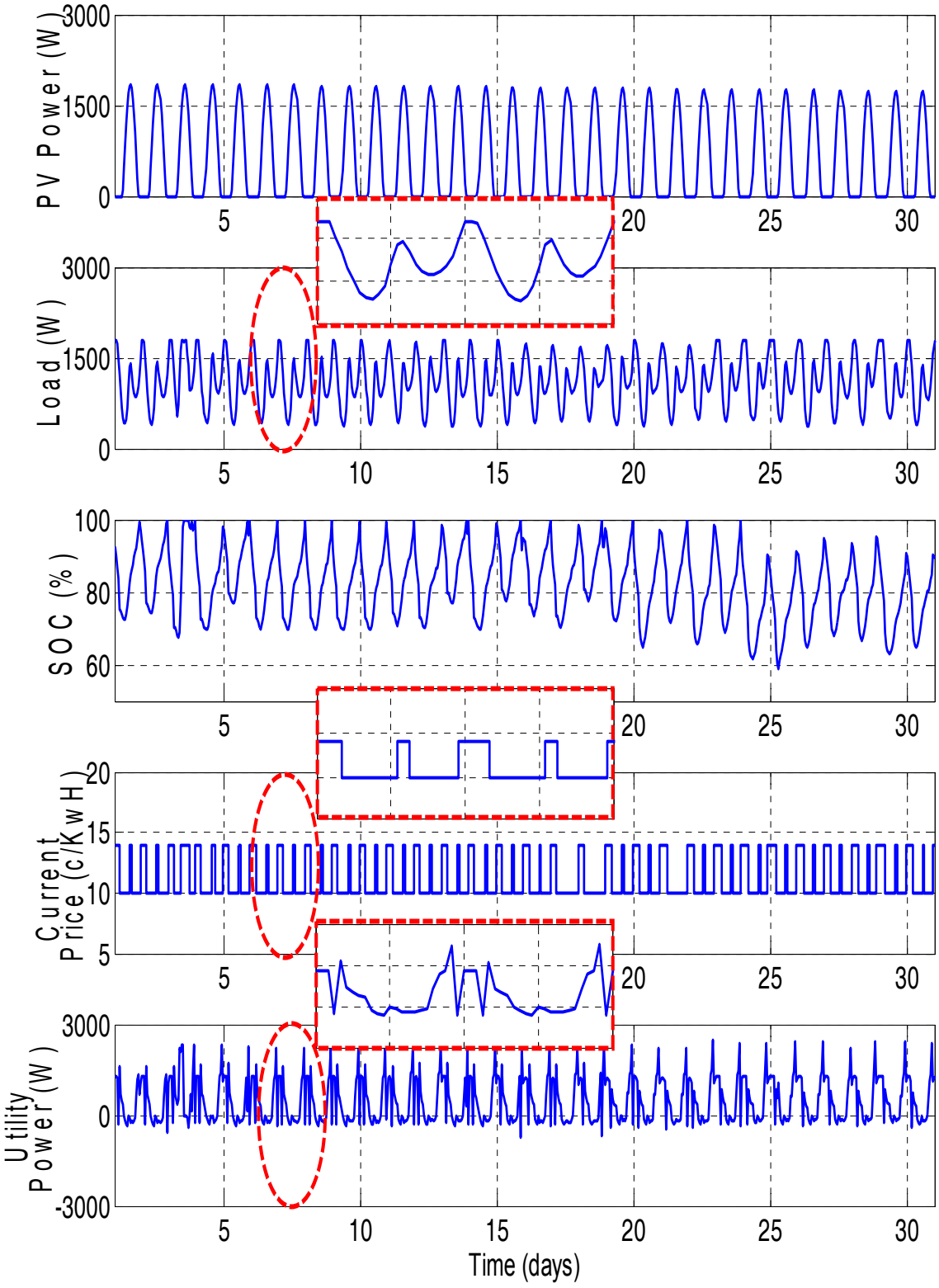


Figure 9.11: Summer Real-time Pricing without Optimized Parameters

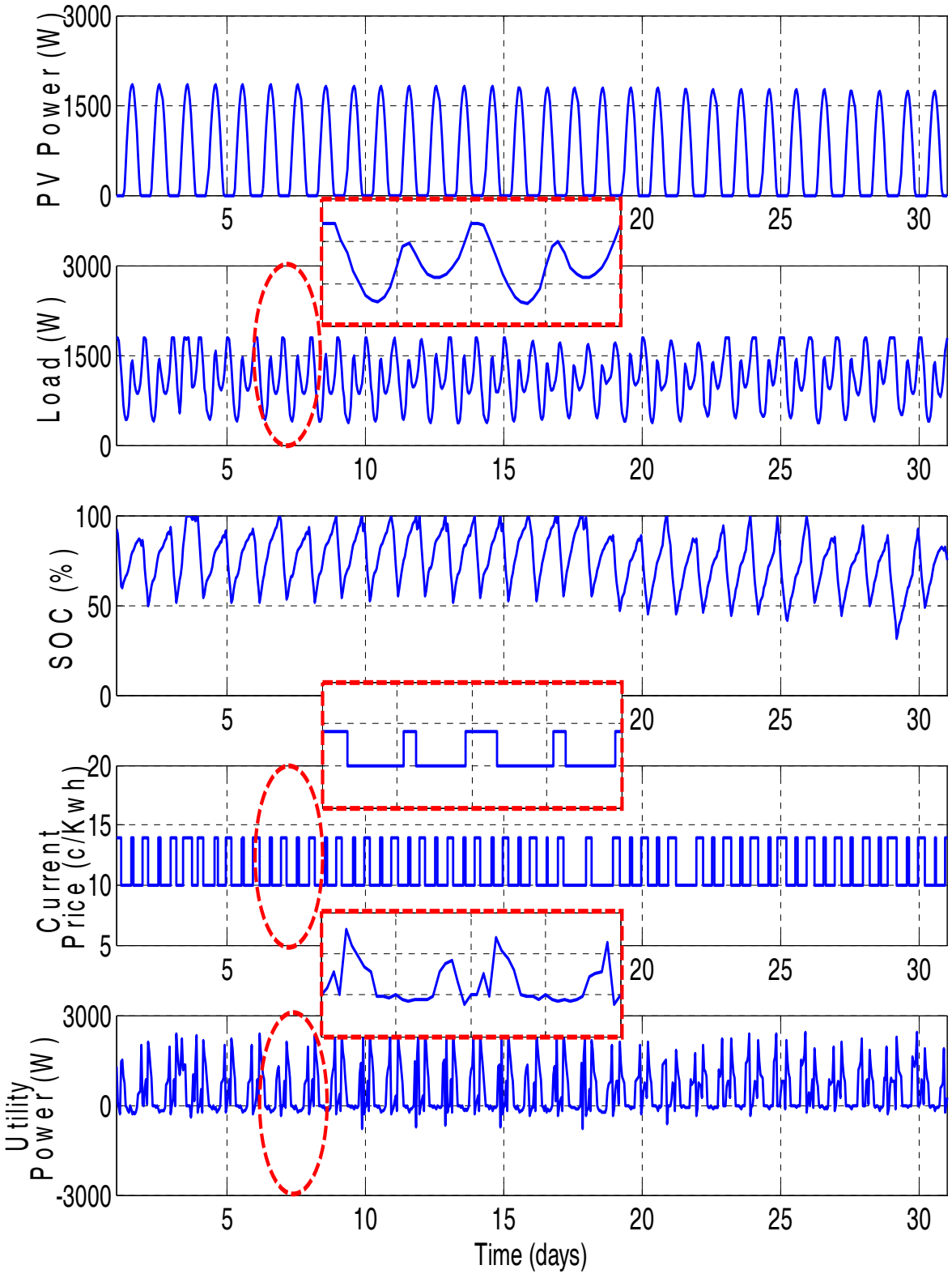


Figure 9.12: Summer Real-time Pricing with Optimized Parameter

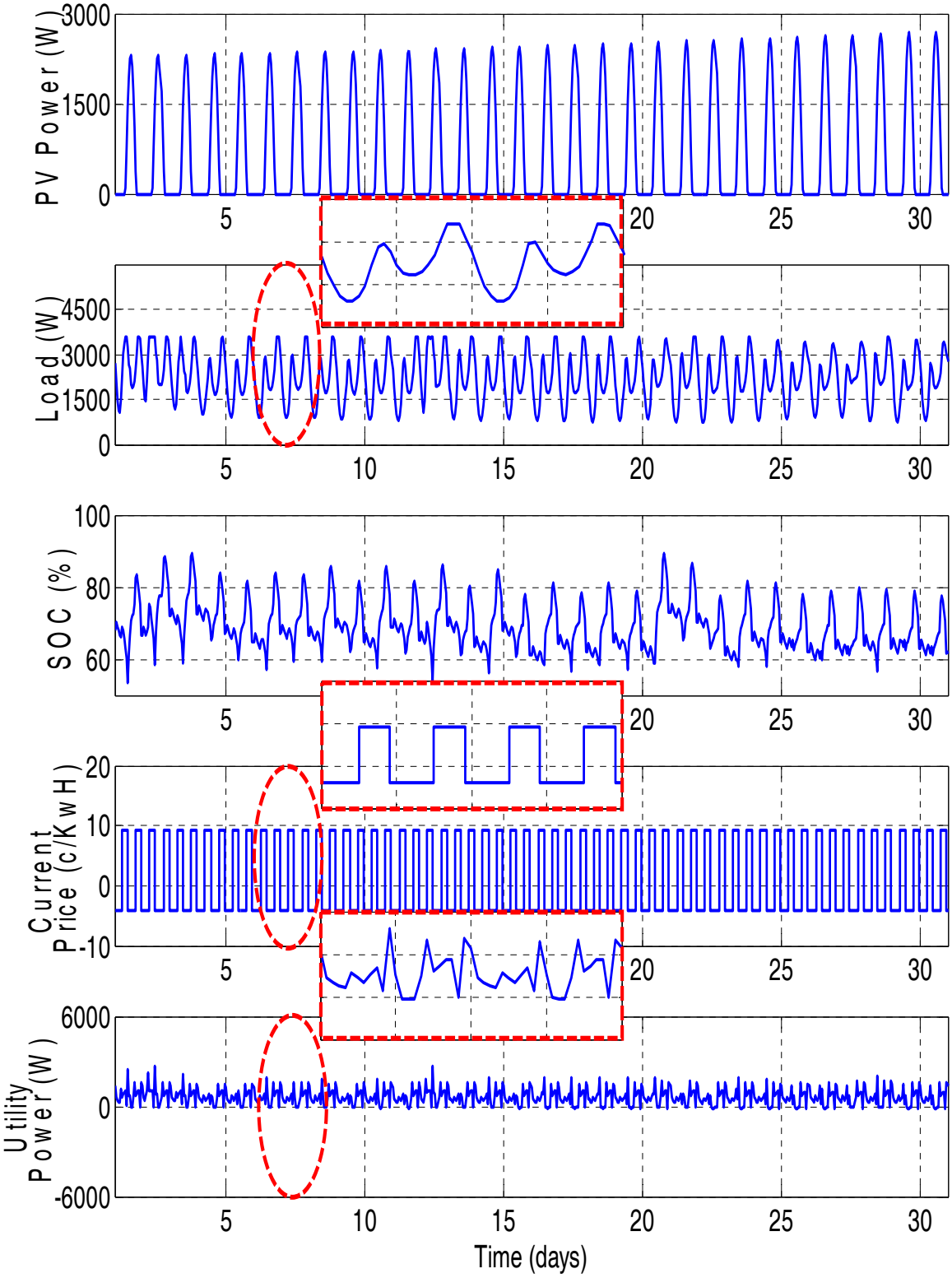


Figure 9.13: Winter TOU Pricing without Optimized Parameters

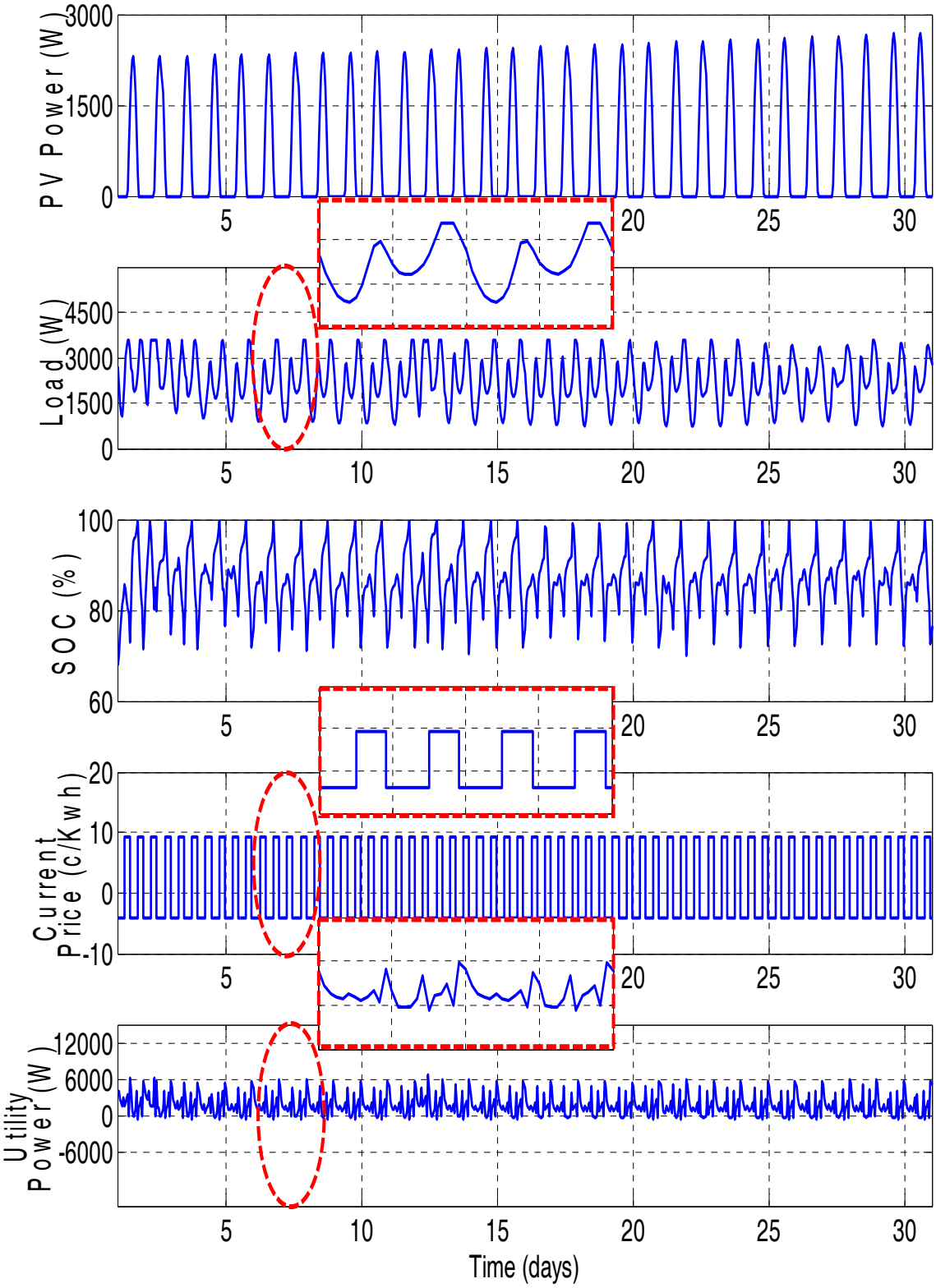


Figure 9.14: Winter TOU Pricing with Optimized Parameters

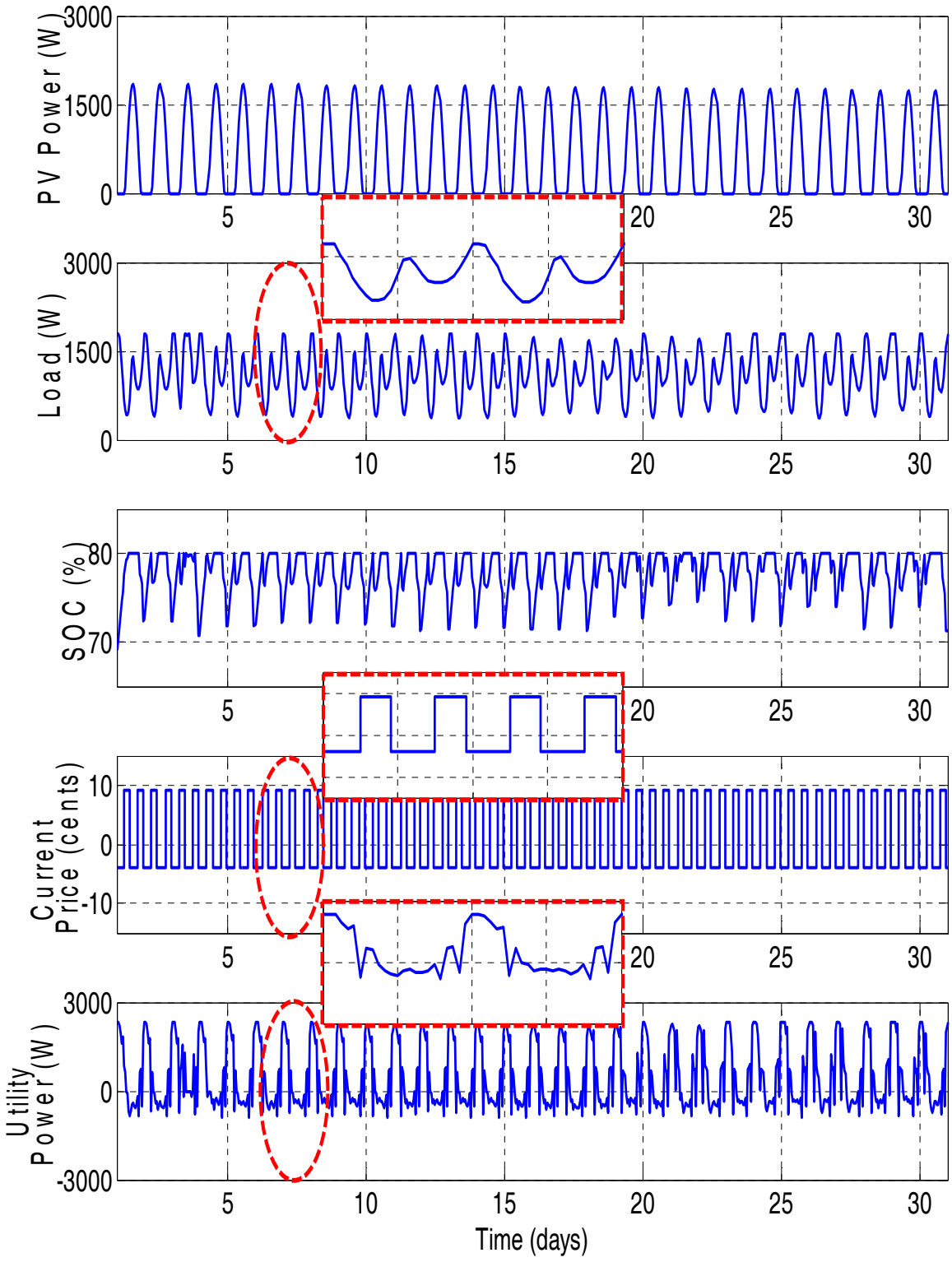


Figure 9.15: Summer TOU Pricing without Optimized Parameters

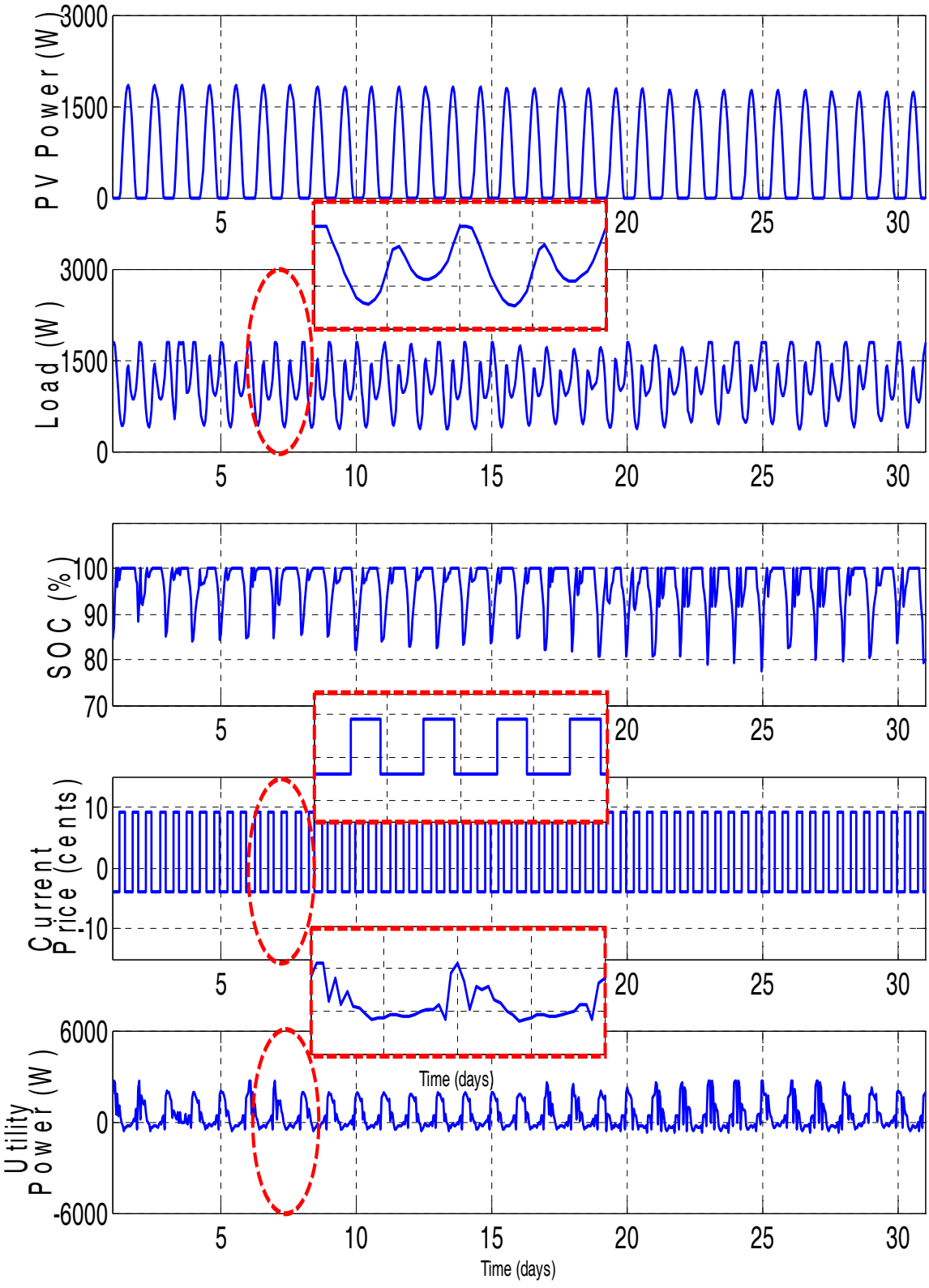


Figure 9.16: Summer TOU Pricing with Optimized Parameters

9.7 Summary

In this chapter, an energy management system for microgrids with an online optimization module accounting for history, current, and future system observations was developed and tested. The communication requirement for each module of the developed EMS (smart meters, load forecasting, controller, etc.) was studied and the required QoS profiles were defined accordingly. The DDS middleware was selected as the communication backbone for the proposed framework for its robust failover mechanisms and a rich set of QoS profiles. A hybrid exploration simulation framework, which exchanges data over a real Ethernet network, was developed to study the sensitivity of the system to networking issues, such as transmission delays, data availability, and reliability among other factors. The EMS was exposed to actual residential energy consumption and irradiance data from Miami, Florida and proved its effectiveness in reducing consumers' bills and achieving flat peak load profiles.

Chapter 10 Load Signature and Customer Privacy

10.1 Introduction

The advanced metering infrastructure (AMI) and other communication technologies will improve the operation of the smart grid. However, this will introduce privacy concerns to customers[102]-[106]. The AMI collects accurate load consumption data from users in a timely manner. This data could reveal some private information about the customer behavior to an observing entity. For instance, by observing the load consumption for a certain period, one could infer and interpret the patterns in a customer's behavior. The energy management system discussed earlier could mitigate this by modifying the load consumption patterns through utilization of energy storage and local energy sources. However, the camouflage in the load pattern provided by the energy management system will not hide all the information that can be used to predict the customer's behavior. For instance, most modern appliances and industrial loads are interfaced with power electronic switching devices. The power electronic interface of these devices creates a voltage and current harmonic signature for each load. These signatures will remain in the load current even after implementing the energy management system. Non-intrusive Load Monitoring (NILM) techniques can track the operation of individual devices by analyzing voltage and current waveforms for these signatures[103].

The NILM is categorized based on the sampling frequency to low and high sampling devices. The low-frequency type samples the power consumption at 1 Hz or lower frequency then maps the changes in the ΔP-ΔQ Plane to extract the power

signature[103][104]. The high sampling NILM type samples the voltage and current at a relatively high sampling rate to capture the harmonic contents of the load current then the captured data was analyzed to identify the harmonic signature for each appliance. An artificial intelligent technique such, as artificial neural network, can be used to extract the harmonic signature [105].

Using the devices' harmonic signature, NILM can construct a database[106] that includes different types of loads and devices operating at the customer's end. Specific operation periods of each load type can therefore be deduced, revealing private customer behavioral patterns as well as the type of equipment used and or owned. For residential customers, one could infer from this data the time in which the customer was in his/her home and operates exactly which appliance (e.g. TV, washing machine …). For industrial facilities, NILM can lead to information leakage about specific types of machines used in production and their operation time. A deep analysis of this information could lead to predicting the production capacity of this company and type of product manufactured. This is critical information in current competitive markets. Finally, NILM is quite a huge concern for military bases located in foreign lands and connected to their utilities. NILM could leak private information about the activities of these military bases and equipment owned by them. As such, compensating for harmonics and reactive power is not only important for the power quality enhancement, but also for ensuring customer privacy. Changing harmonics and power signature can improve the customer's privacy and prevent NILM techniques from revealing private information from consumption measurement. Different approaches were developed to compensate for reactive power

and reduce harmonics [107]-[113]. Changing the harmonic signature for multiple appliances requires online analysis for the current and automatic compensation for harmonics. In this chapter, the shunt Active Power Filter (APF) control algorithm will be proposed to change the load signature and improve the power quality for a group of connected loads. Moreover, the proposed APF control algorithm can inject a fake signature to disturb NILM.

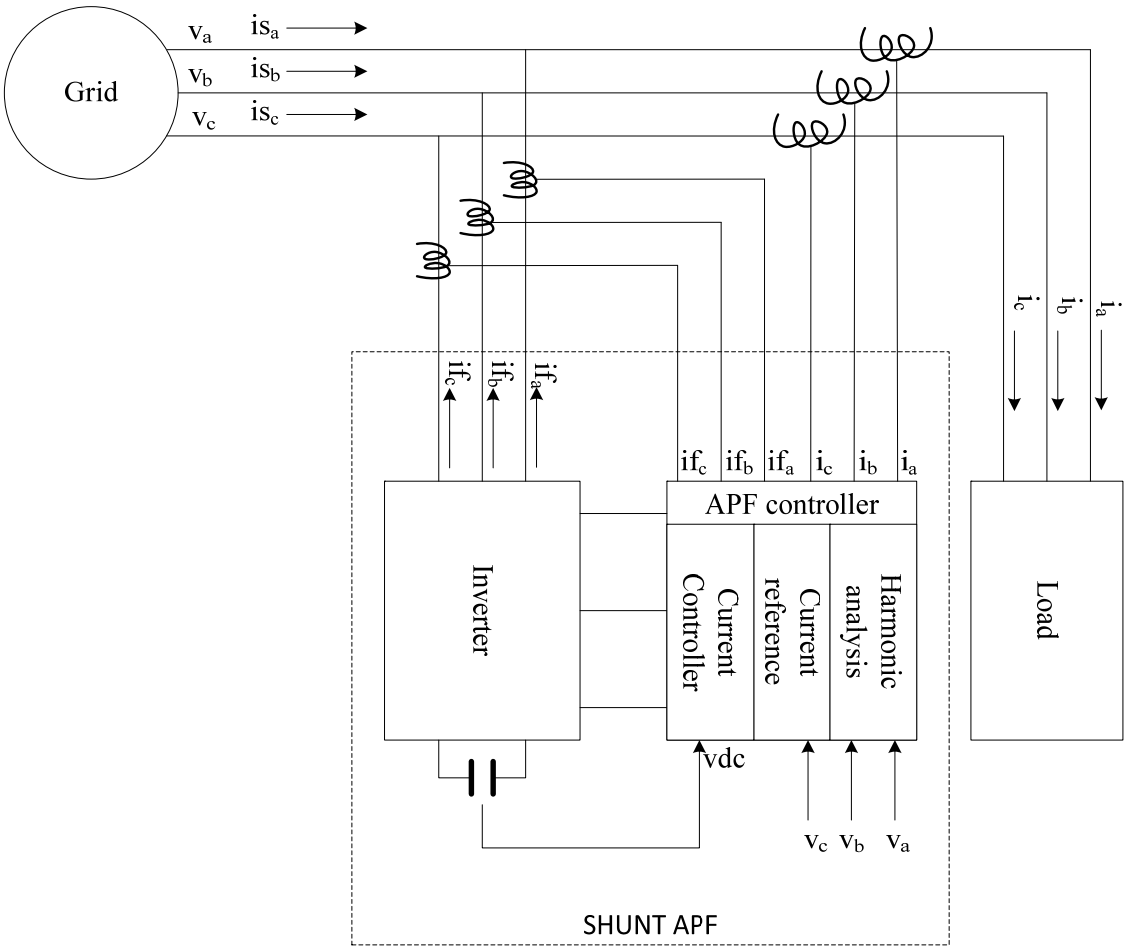


Figure 10.1: shunt active power filter block diagram

APF can be connected in shunt or series. Shunt APF provides the capability to compensate for harmonics and reactive power simultaneously [114]. Moreover, the

proposed active power filter can also compensate for unbalanced loads. Compensation for unbalanced load current makes it difficult for NILM to distinguish between single-phase and three-phase loads. The APF controller analyzes the load current in real-time to extract a reference current that represents the harmonics and reactive current components and injects an opposite current to cancel unwanted components from the source current, as shown in Figure 10.1.

The performance of the active filter is mainly dependent on the accuracy of the used method to extract undesired harmonic component and the current controller that inject the current with opposite the direction to cancel the unwanted component. The Synchronous Reference Frame (SRF) method was used to extract the undesired current in three-phase balanced systems, but it fails with an unbalanced system. While instantaneous power theory is usually used in the three-phase four-wire unbalanced systems, the disadvantage of instantaneous power theory is that it requires measuring the voltage and current for the three phases and requires more computations, which are reflected in the costs of implementation. The harmonic extraction methods and current controller will be discussed in detail in the next sections

10.2 Harmonic and reactive current extraction

The first stage in the APF control is the generation of a reference current that represents harmonics and reactive current contents. Calculating the reference current is either based on frequency or time domain. The frequency domain compensation is based on Fourier analysis of the distorted signal to extract the harmonics, which leads to high computation burden and slow response. The time domain compensations are based on the

instantaneous derivation of the compensating signals from the distorted ones. Most of the time domain compensation techniques are based on the synchronous reference frame and instantaneous power theory.

10.2.1 Synchronous Reference Frame Current Reference Generation Method

The synchronous reference frame compensation method uses the Park's transform to represent the distorted signal in the d-q plane, as depicted in equation (10.1). With this transformation, the fundamental component will be represented by a DC value in the d-q plane. The harmonic component will be represented by an AC component with a frequency of 120 Hz and/or other multiples of 60 Hz. The active power, in this case, corresponds to the component of the current in the d-axis, while the reactive power corresponds to the other component. The harmonic compensation current can be extracted from the d-axis current using a high-pass filter as shown in Figure 10.2. In the case of a three-phase unbalanced system, when applying Park's transform, an AC component appears in the d-q plane with a frequency of 120 Hz in 60 Hz networks due to unbalancing. This AC component is equal to the AC component produced by the third harmonics[115] which leads to injection of 3rd harmonic to the grid.

$$\begin{bmatrix} i_0 \\ i_d \\ i_q \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ cos\,\theta & cos\left(\theta - \frac{2\pi}{3}\right) & cos\left(\theta + \frac{2\pi}{3}\right) \\ -sin\,\theta & -sin\left(\theta - \frac{2\pi}{3}\right) & -sin\left(\theta + \frac{2\pi}{3}\right) \end{bmatrix} . \begin{bmatrix} i_a \\ i_b \\ i_c \end{bmatrix} \quad (10.1)$$

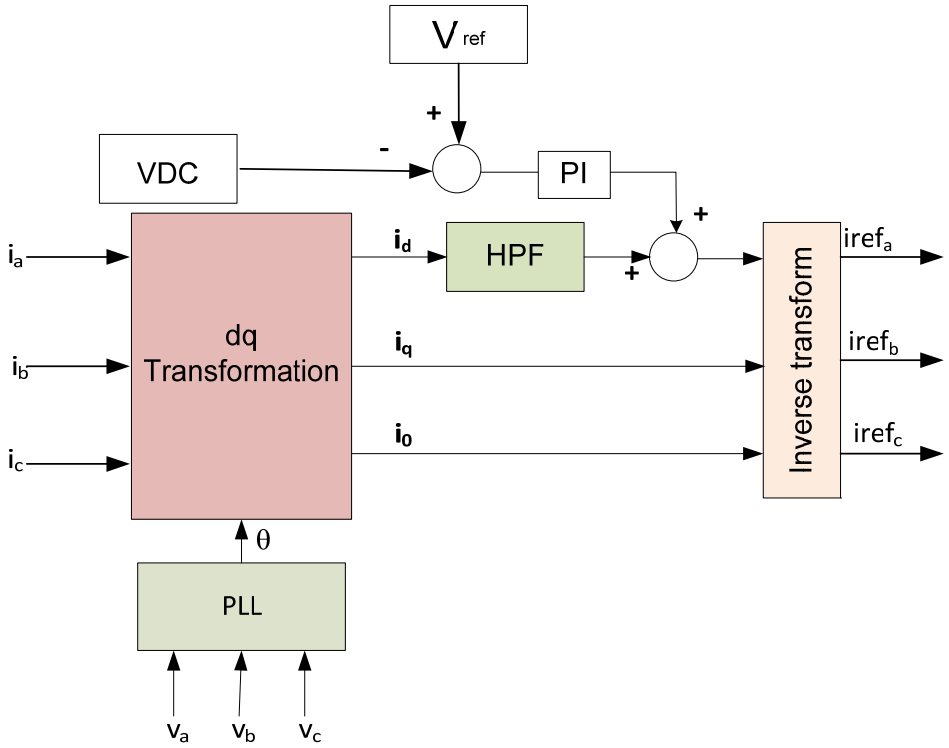


Figure 10.2: Block diagram of synchronous reference frame reference generation method

10.2.2 Instantaneous Power Theory reference generation method.

To overcome third harmonic injection due to the unbalanced condition, the harmonic component can be extracted using the instantaneous power theory proposed by Akagi [116],[117]. This method is based on Clark's transformation of the three-phase voltages and currents from the ABC coordinates to the αβ0 coordinates. The AC and DC components of the power can be obtained from the instantaneous values using high-pass and low-pass filters, respectively, as depicted in Figure 10.3. The instantaneous power theory can be applied to three-phase four-wire balanced and unbalanced systems. It can also be applied to a system with voltage harmonics [118]**Error! Reference source not**

found.. However, there are some disadvantages of the instantaneous power theory technique; they involve complex hardware implementation due to the requirement of measuring voltages and line currents, and extra calculations to transform voltage and current to αβ0 coordinates.

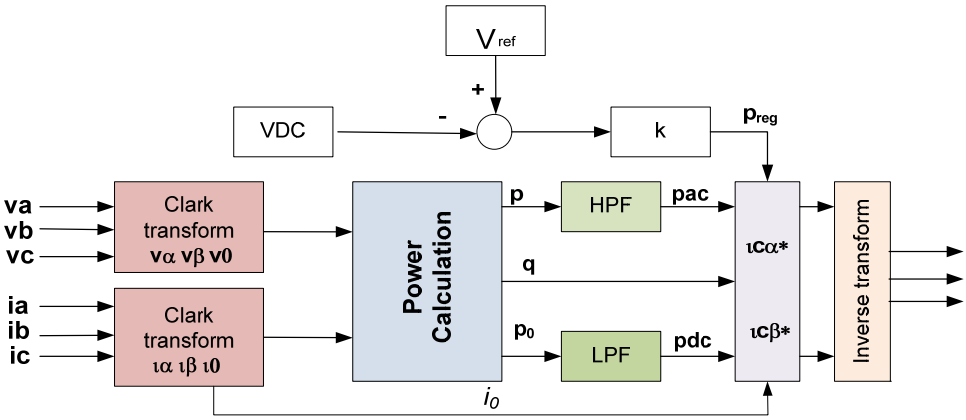


Figure 10.3: Block diagram of Instantaneous Power Theory reference generation method

10.2.3 Proposed current Reference Generator

In the proposed method, the harmonic current was extracted from the measured load current through the use of a modified synchronous-reference frame-based method. The synchronous reference frame method requires measuring the three-phase load currents only rather than the three-phase currents and voltages in the instantaneous power theory-based method. The disadvantage of the synchronous reference frame-based method is that it is only suitable for a three-phase balanced system. Accordingly, some modification will be presented herein to make it suitable for three-phase, four wires, balanced and unbalanced systems. Figure 10.4 shows the block diagram of the modified synchronous

reference current generator. The direct current id is being calculated from the three-phase current using Park's transformation.

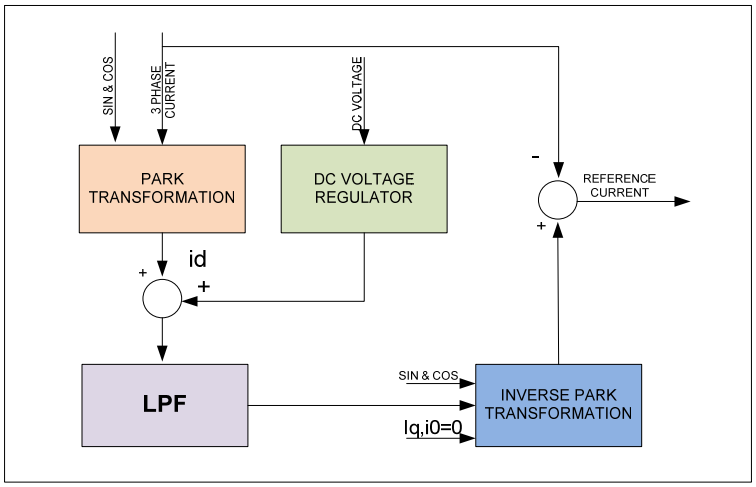


Figure 10.4: A block diagram of the reference current generator

The calculated id contains a DC component that represents the fundamental active component current, while the AC component represents the harmonic components. The AC component frequency will be 120 Hz in an AC 60 Hz network and 100Hz in an AC 50 Hz network. To obtain the DC component, id passes through a low-pass filter with a cutoff frequency of 75 Hz. The output of the low pass filter will represent the fundamental active current component. The filtered id will be used to obtain the sinusoidal fundamental component existing in the load current by using inverse Park's transform. iq and i0 will be set to zero since we need to obtain the active fundamental component only. Consequently, the calculated sinusoidal component is subtracted from the load current. The obtained component is a reference current that represents all harmonics and reactive components existing in the load current. By this method, we can manage to overcome the problem of the AC component that exists in the id current due to the unbalanced load, since calculations in this scheme depend on calculating the

fundamental component existing in the load current. Hence, it is being subtracted from the load current to obtain the distorted component instead of calculating it directly. To calculate the Park's transform, the supply phase angle must be known. A PLL was used to track the supply voltage phase angle in order to calculate sin(θ) and cos(θ) [119]. In some cases, a frequency drift of the fundamental component can occur. The adopted ASRF-PLL has the capability to accurately track the frequency and compensate for this drift.

10.2.4 Active power filter current controller.

After extracting the harmonic and generating reference current for the unwanted component, the next stage is to inject this component with opposite direction to the supply system. Three-phase voltage source converter with self-supported DC bus will be used as a power amplifier to inject the harmonic current, as shown in Figure 10.5 To operate the voltage source converter in current control mode, a hysteresis current controller was used to regulate the injected current.

Hysteresis control provides good harmonic suppression. However, as a disadvantage of such a technique, its switching frequency is not fixed. The power losses in semiconductors increase with increasing the switching frequency, therefore, it is very important to limit the switching frequency in high-power applications to minimize the power losses and increase the efficiency[120].

To overcome the variable switching frequency problem, a modified version of the hysteresis current controller was developed and adopted. In the regular hysteresis controller, the error function is centered in a fixed pre-set hysteresis band. When the error

exceeds the upper or lower hysteresis limits, the hysteresis controller makes an appropriate switching decision to control the error within the pre-defined band. To limit the maximum switching frequency, another limiting stage was added to the controller.

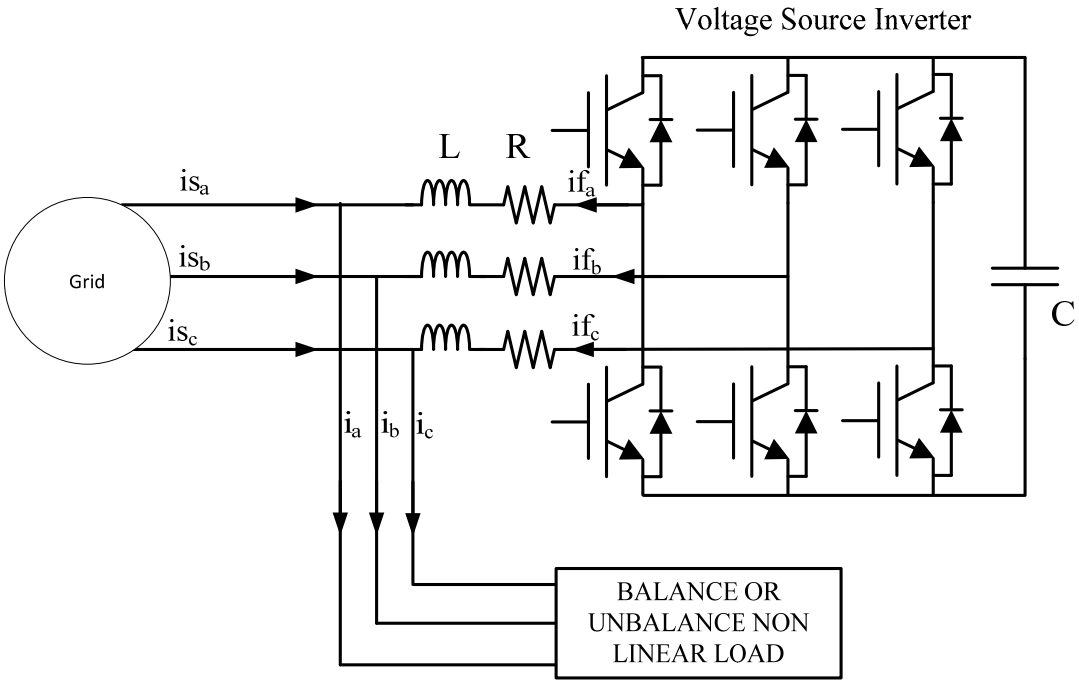


Figure 10.5: Voltage source inverter with self-supported DC bus

This limiting stage consists of an edge triggered flip-flop and a controlled oscillator. Figure 10.6 shows a block diagram of the developed hysteresis controller. When the switching frequency exceeds the maximum limit, the flip-flops and oscillator override the controller command and limit the output frequency; this will lead to increasing the hysteresis band in accordance with limited switching frequency. As shown in Fig. 6, i^* is the reference current calculated by the reference current generator and i_{inv} is the actual current injected by the voltage source inverter. The f_{max} signal fed from an oscillator with

a frequency that equals the desired maximum switching frequency.

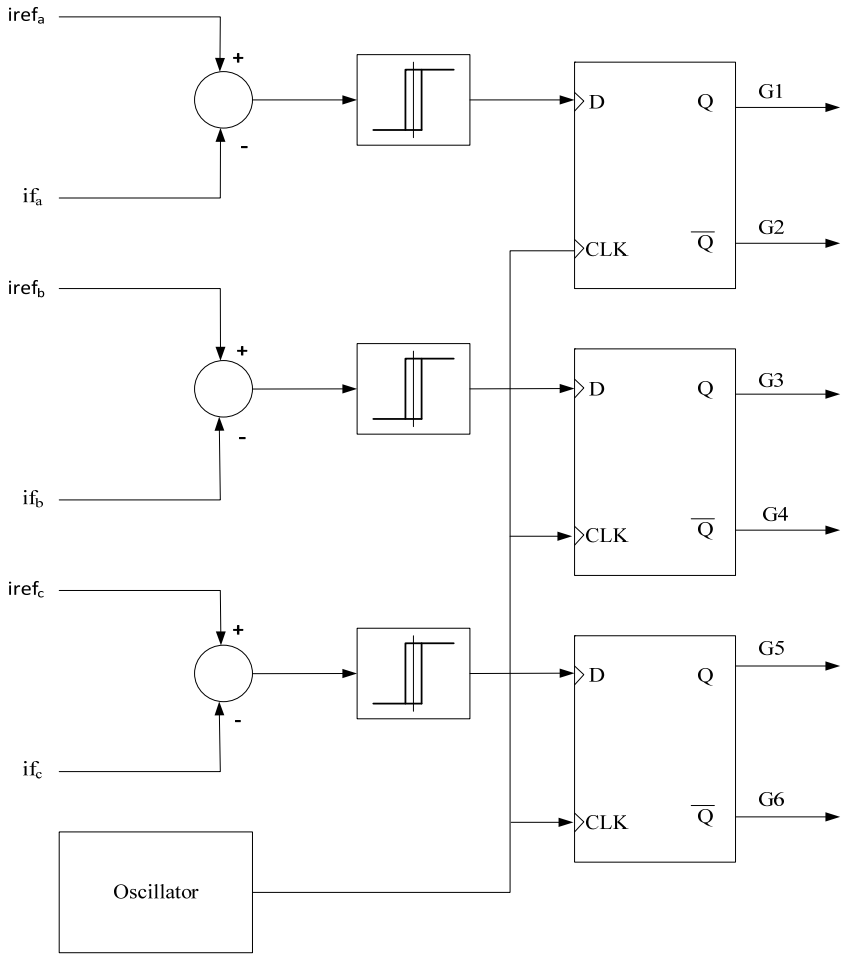


Figure 10.6: A block diagram of the developed hysteresis controller

10.3 Case studies

To investigate the efficiency and ability of the proposed control technique to change the load signature, APF was tested with four different operation cases. The first test case involves dynamic inductive load to test the ability to hide the reactive power signature with sudden load change. The second test case involves unbalanced load to demonstrate the ability to hide the signature of a single-phase load connected to three-phase networks. The third test case shows the change in the harmonic signature for the nonlinear load. The

fourth test case demonstrates the ability of the APF to inject harmonic that emulates nonlinear load signature. The control of the APF filter was deployed using a dSPACE-1104 embedded controller. The power circuit for the APF was implemented using a three-phase power electronics converter, shown in Figure 10.7. The converter was connected to the grid through 24mH inductors. The hysteresis current controller was limited to 20 KHz switching frequency.

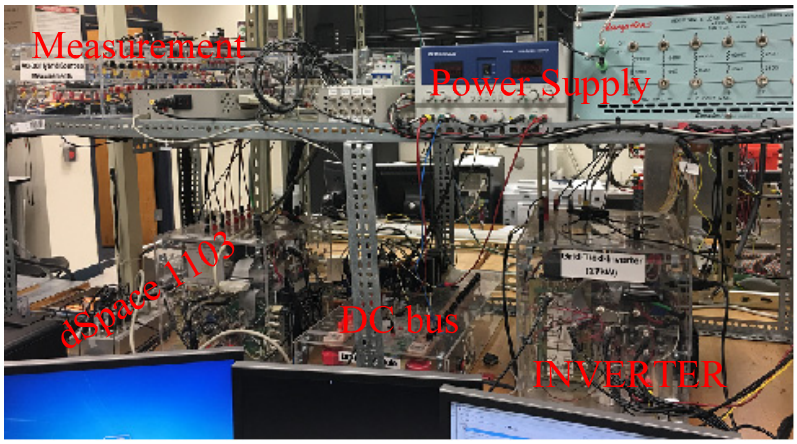


Figure 10.7: APF hardware setup

10.3.1 Case Study one: Three phase dynamic inductive load.

In this case, three-phase load consumes 900W active power and 300VAR reactive power is connected to the three-phase supply. The APF was connected in parallel with the load to compensate for reactive current, as shown in Figure 10.8. At time equal to 0.1, sec the load changes to 1200W and 300VAR. The APF smooths the sharp change in the supply current results from sudden load change, as shown in Figure 10.9. Sharp changes are necessary for NILM meters to detect the start and stop instances of appliances. Smoothing these edges reduce the ability of NILM to detect the starting of new devices. To hide the reactive power signature, the APF succeeds to maintain unity power factor

during steady state and load transient. Figure 10.10 shows the phase angle between the supply voltage, the load current and supply current. The load current has a phase delay with respect to the supply voltage while the supply current maintains a zero phase angle during the test period.

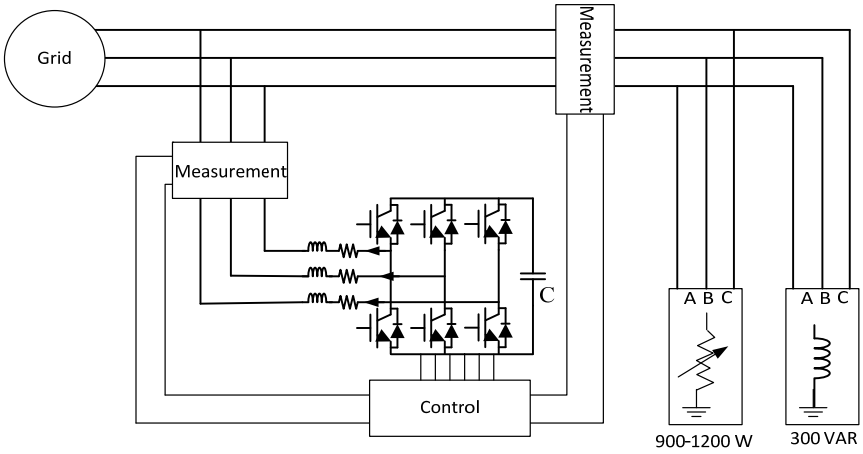


Figure 10.8: Three phase dynamic load with shunt APF connection diagram

10.3.2 Case Study two: Three phase unbalanced inductive load.

To demonstrate the APF compensation for the unbalanced current, the three-phase unbalanced load was connected parallel to the APF. The balanced load draws 300W from phase a, and 420W from phase b and c. All phases are loaded with 100VAR reactive power. Figure 10.11 -a and 11-b shows the supply voltage and unbalanced load current, respectively. As depicted from figure 11-c, the APF distributes the consumed energy between the three phases and the supply current becomes balanced. Also, the APF maintains a zero-phase angle between the supply voltage and current, as depicted in Figure 10.12.

10.3.3 Case Study three: Three phase nonlinear load with harmonic current.

In this case, the APF will be connected in parallel with the group of loads. The loads consist of three-phase inductive load and unbalanced load demonstrated in the previous case. Additional three-phase rectifier with RL load is connected in parallel. It is known that due to the uncontrolled operation of the diodes, the uncontrolled rectifier injects harmonics to the system. Figure 10.13 (a), (b), and c show the supply voltage, load current and supply current, respectively. The load current shown in figure 13 (b) has 5^{th} and 7^{th} harmonic with 6.51% and 4.46%, respectively. As depicted from figure 13 (c), the proposed APF control algorithm succeeds to compensate for the unbalance and harmonic current. The supply current has 5^{th} and 7^{th} harmonic with 1.27% for both harmonic components. Another merit of the proposed technique is the compensation for reactive power, as shown in Figure 10.14. As depicted from figure 14 (b) and 14 (c), the proposed algorithm compensates for the reactive power and maintains a zero-phase angle for the supply current.

10.3.4 Case Study four: Emulating a nonlinear load current signature.

In addition to removing load current signature, APF can emulate harmonic and reactive power signature for a nonlinear load. By emulation load signature, the APF can deceive the NILM to detect non-existing loads. In this case, a three-phase load with 900W and 300VAr was connected to the three-phase supply. The shunt active power filter was used to emulate the harmonic signature for a three-phase rectifier feeding RL load. The APF current reference generator was programmed to inject 5^{th} and 7^{th} harmonic. The supply voltage, load current and supply current are shown in Figure 10.15 (a), 15 (b) and 15 (c),

respectively. As depicted from Figure 10.15 (b), the load current was pure sinusoidal with no harmonic content. The supply current shown in Figure 10.15 (c) has 5^{th} and 7^{th} harmonic orders with 6.85% and 4.17%, respectively. The injected harmonics current mimic the signature of the uncontrolled rectifier used in the previous case. It is worth to note that, the harmonic injected by the APF to emulate a load signature should not exceed the limits specified by the standard.

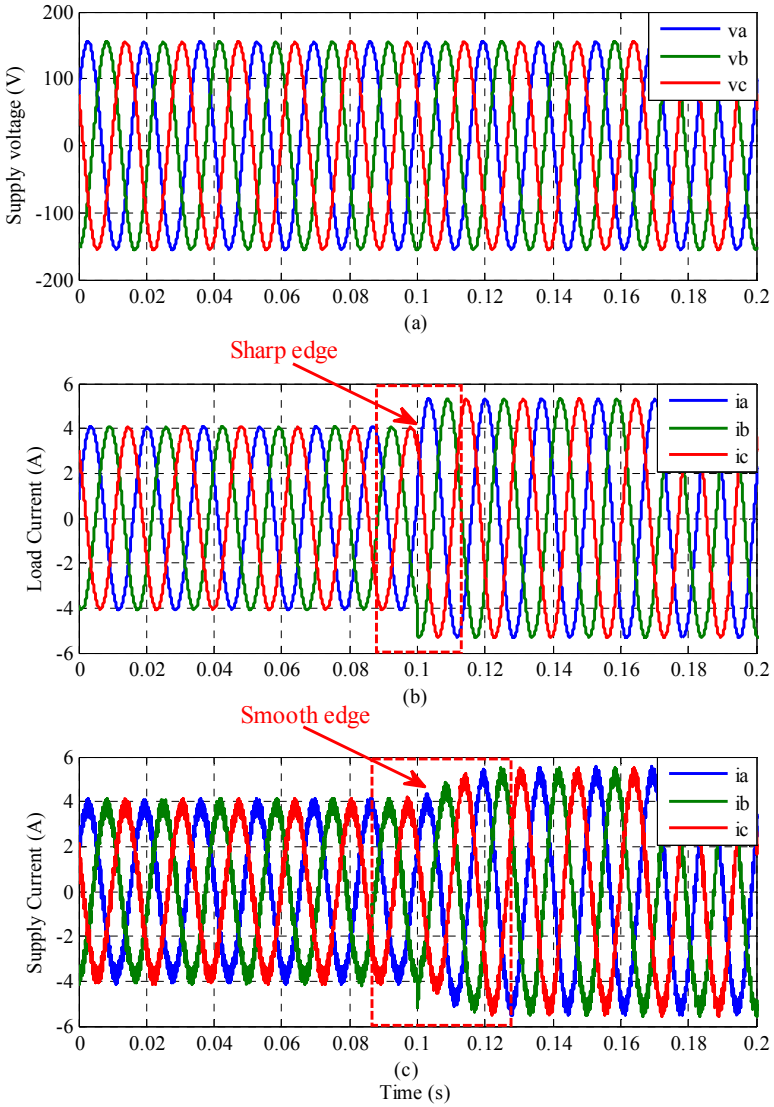


Figure 10.9: APF performance with the three-phase dynamic load. (a) Supply voltage, (b) Load current, (c) Supply current

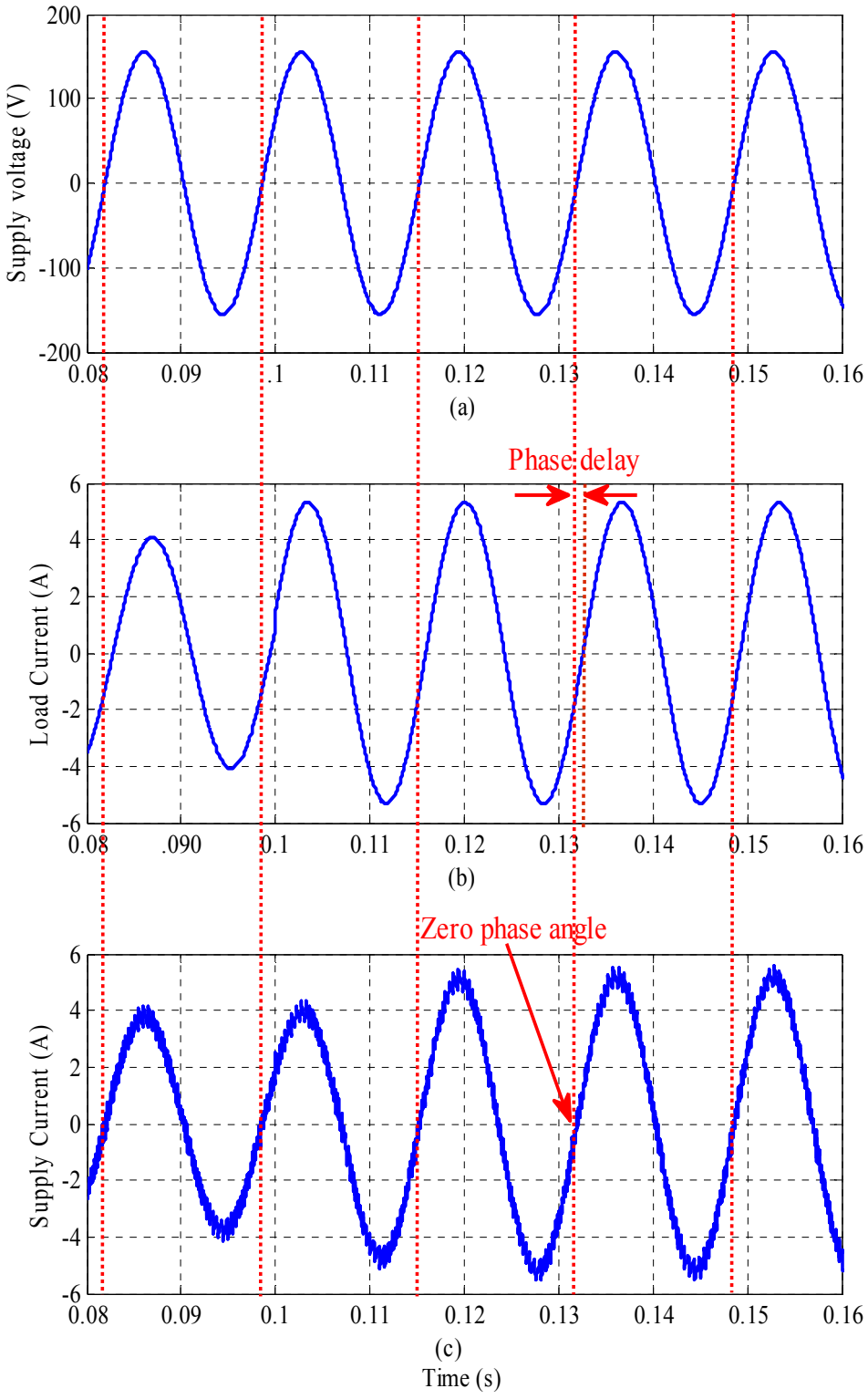


Figure 10.10: Dynamic load and supply current phase angle. (a) Supply voltage, (b) Load current, (c) Supply current

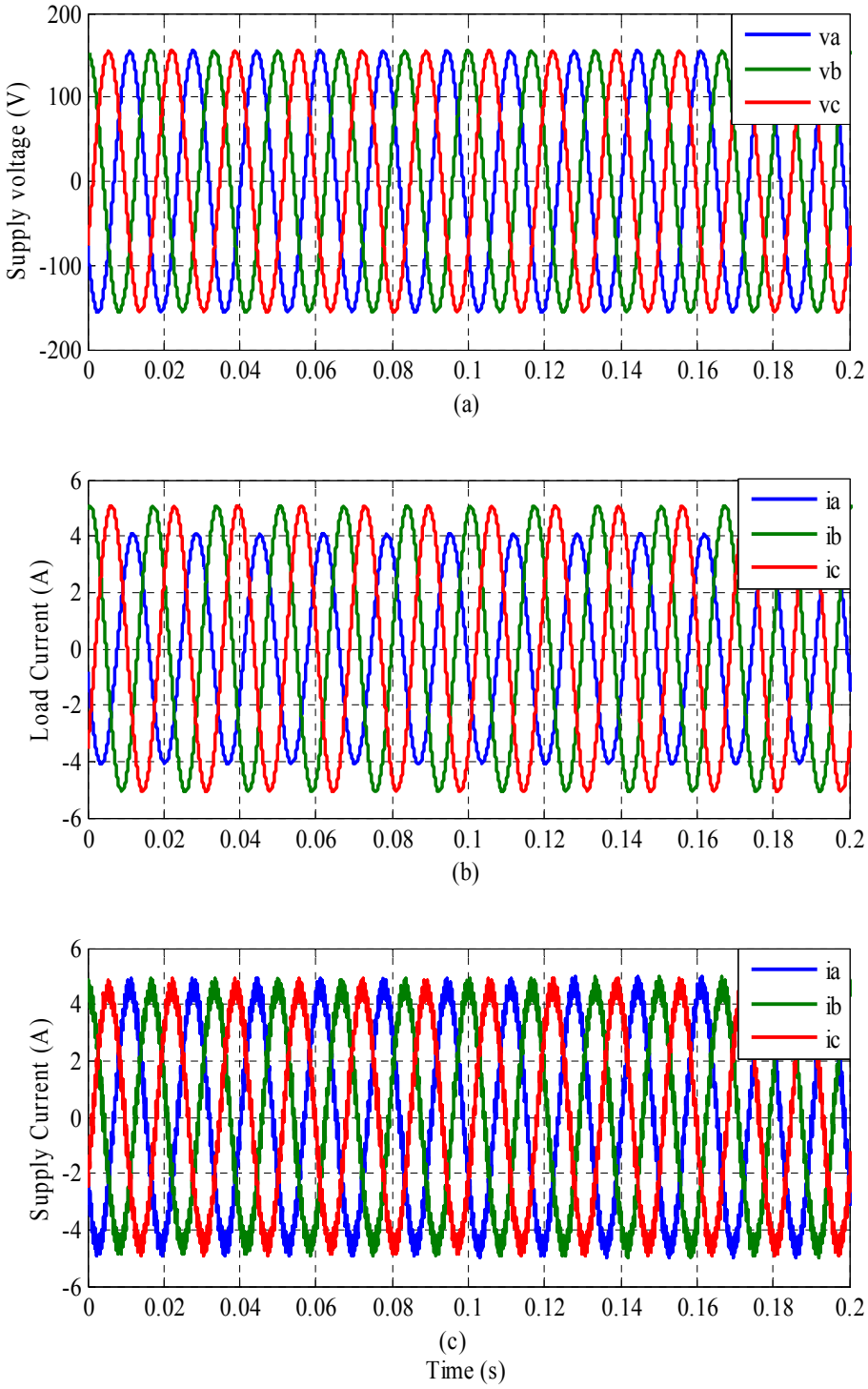


Figure 10.11: APF performance with three phase unbalanced load. (a) Supply voltage, (b) Load current, (c) Supply current

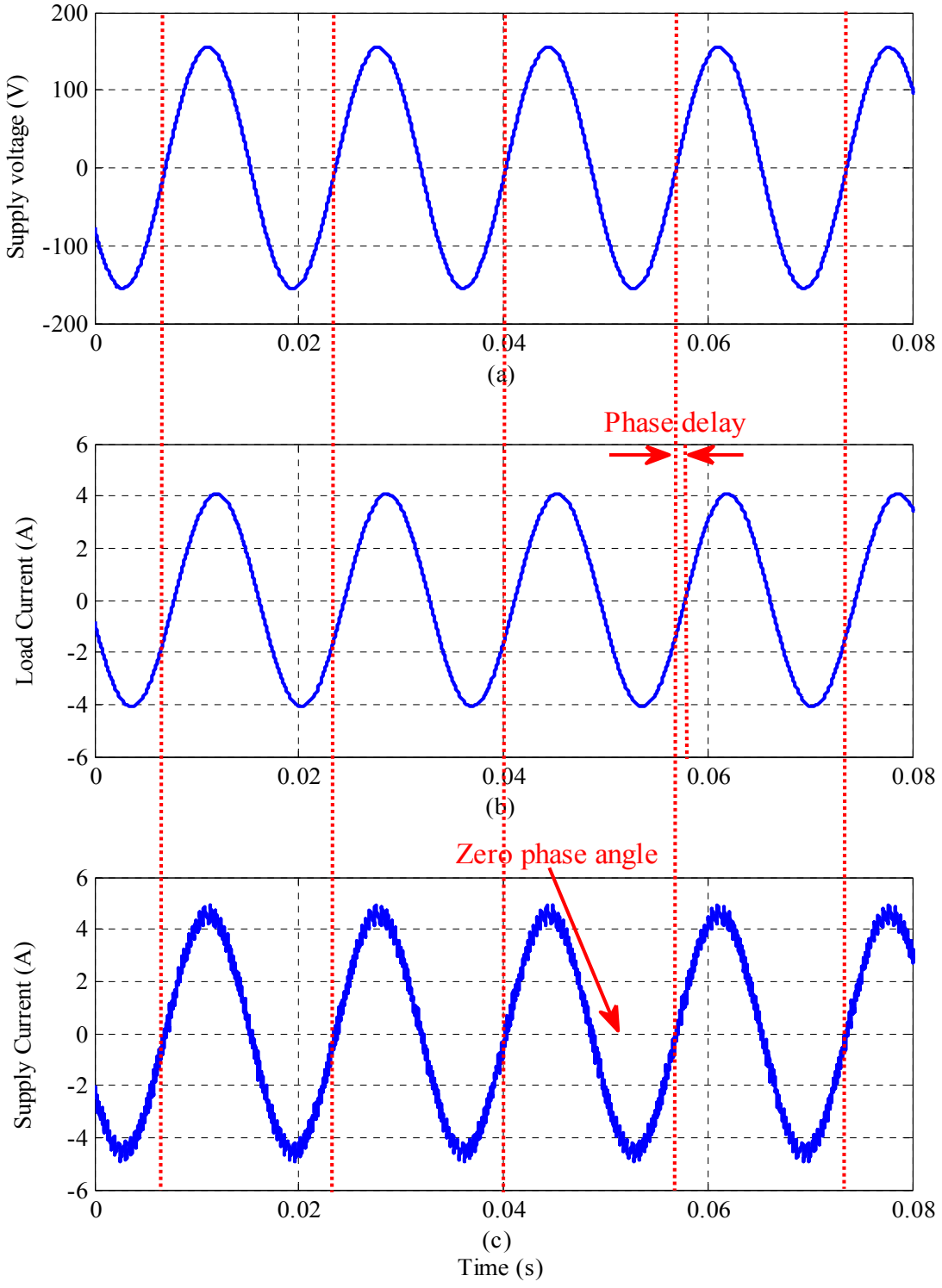


Figure 10.12: Unbalanced load and supply current phase angle. (a) Supply voltage, (b) Load current, (c) Supply current

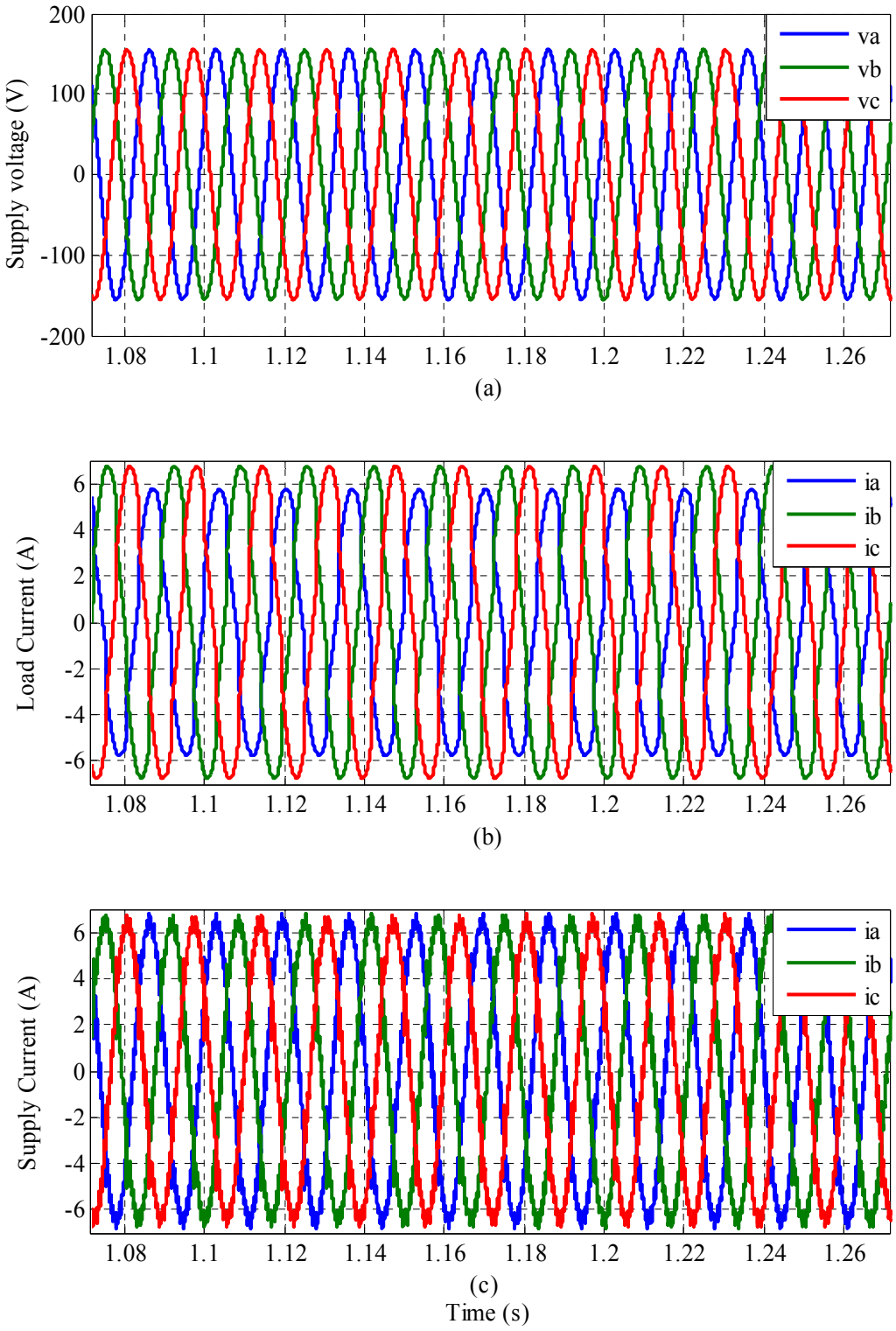


Figure 10.13: APF performance with three phase non-linear load. (a) Supply voltage, (b) Load current, (c) Supply current

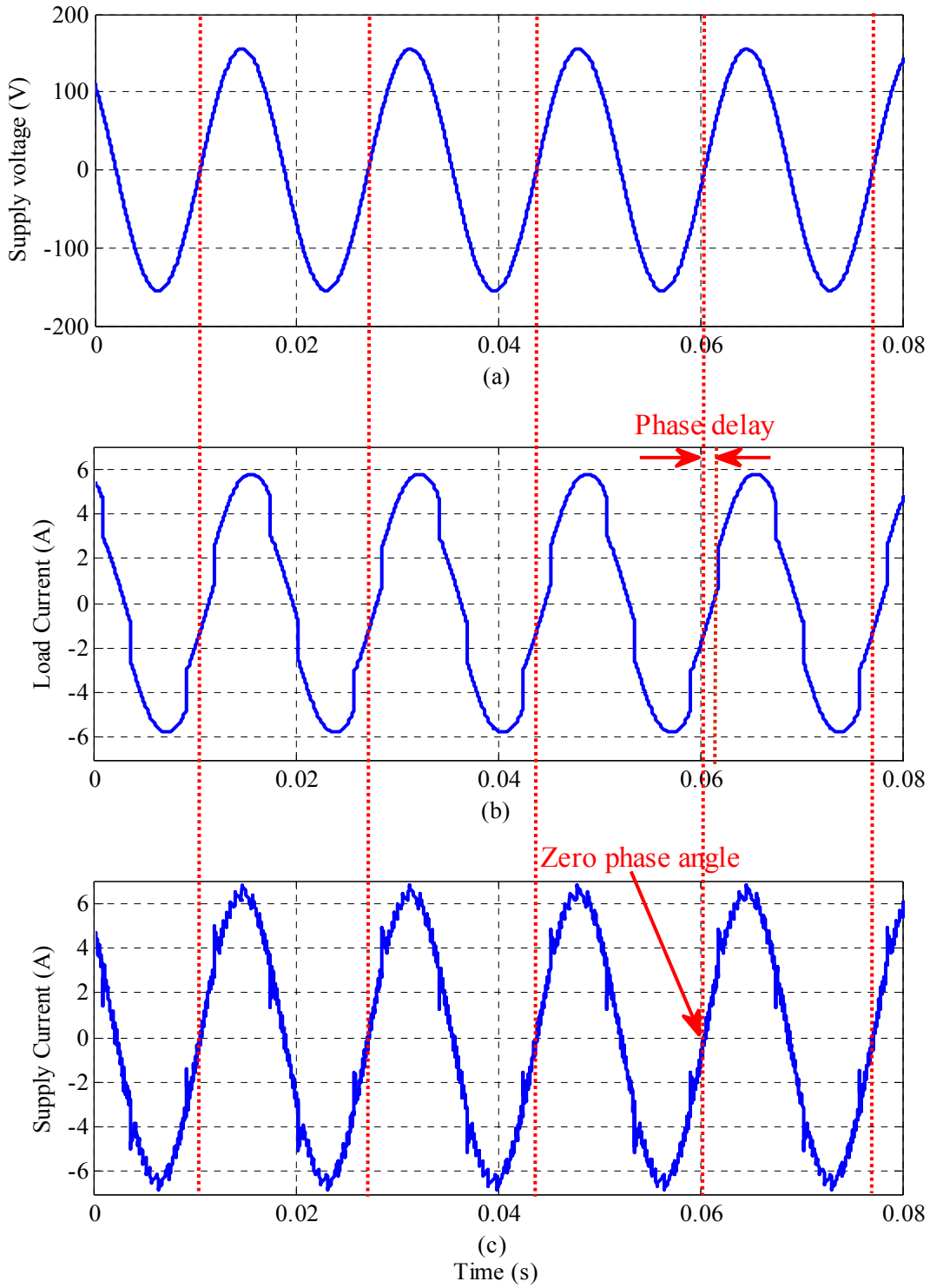


Figure 10.14: nonlinear load and supply current phase angle. (a) Supply voltage, (b) Load current, (c) Supply current

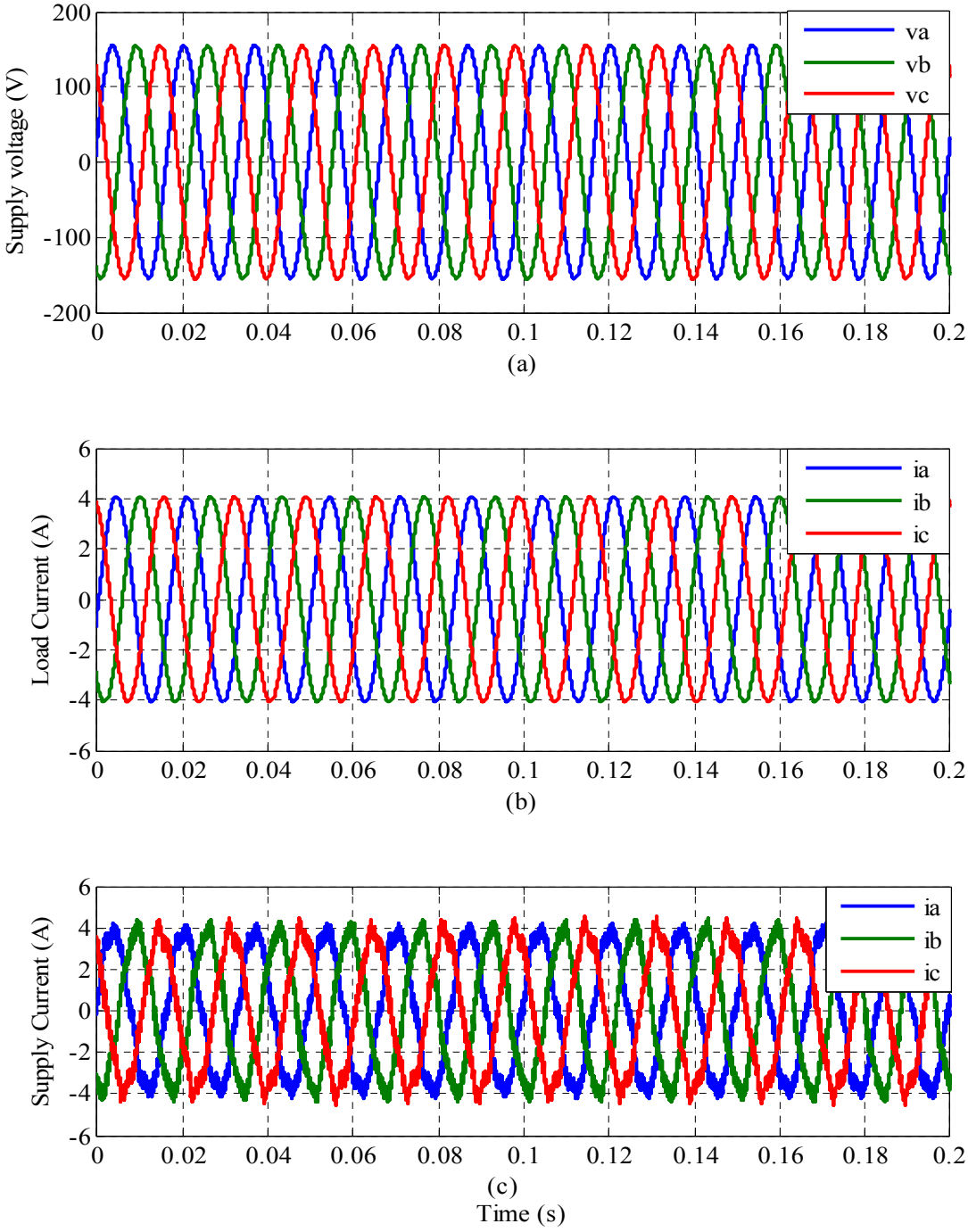


Figure 10.15: Load signature emulation. (a) Supply voltage, (b) Load current, (c) Supply current

10.4 Summary

In this chapter, a synchronous reference frame-based controller was modified to be adequate to operate with balanced and unbalanced loads. This controller was used to control APF to compensate for current signature and different power quality issues for both balanced and unbalanced non-linear loads. Also, a modified version of the hysteresis controller was presented to overcome the problem of variable switching frequency and to appropriately control the switching frequency. The proposed control algorithm was experimentally tested to verify the effectiveness of the system. Different loading conditions were tested to verify the effectiveness of the system. The loading conditions were selected to represent different types of load signature. The test results show that the controller deals automatically and successfully change the load current signature, which improves the customer privacy by deceiving NILM. The proposed controller requires less computation compared to instantaneous power theory and regular synchronous reference frame methods. Combining the proposed active power filter control with energy the management system improves the customer privacy, in addition to reducing the energy cost and improves the power quality.

Chapter 11 Electromagnetic Signatures

11.1 Introduction

Modern control and design technologies dictate the use of power electronics in various stages of the power system. The electrical systems are becoming increasingly complex, as they are composed of microprocessor circuits, communication circuits, snubber circuits, sensors, among other components. Power electronics interfaces produce voltage and current harmonics; these harmonics radiate a stray electromagnetic field around controlled equipment. A Radiated field can cause electromagnetic interference problems to nearby devices. Moreover, the electromagnetic signature for controlled devices can be detected and identified remotely. Remote identification of equipment's electromagnetic signature raises privacy and security concern for some types of power systems, such as shipboard power system. Shipboard power system represents a microgrid with multiple generators, distribution network, and heavy loads. Detection of electromagnetic signature remotely represents a threat to military ships. The stray field can activate naval mines and reveal location information. Several sources contribute to the ship electromagnetic signature, such as structural ferromagnetic material, cathodic protection and stray field from onboard equipment. The stray electromagnetic field is radiated from heavy current equipment, such as electric propulsion system drive and generators. The stray field can radiate through the ship hull into the surrounding environment and water, which can be detected at a distance. Shielding techniques are used to reduce the electromagnetic signature. By reducing the harmonic component that generates the stray field, especially from motor drives, the shield size can be reduced.

Many valuable strategies are proposed to reduce the harmonics content, ranging from modifying the rotor design [121] to torque reduction [122], revising the control algorithm of the converter [123], [124], and multilevel converters among others. Some researchers utilized artificial intelligence techniques, such as genetic algorithms, fuzzy logic and others in optimizing the performance of multilevel converters, such as in [125], [126], and [127]. In [125], the genetic algorithm optimization was applied to the multilevel inverter to determine optimum switching angle for cascaded multilevel converters. The intention was decreasing higher order harmonic while maintaining the fundamental harmonic. The process of calculating the optimized switching angle is offline. In [127], the authors utilize a hybrid real-coded genetic algorithm for finding the optimal solution to the nonlinear equation system with fast and guaranteed convergence. Different operating points for both five- and seven-level converters, including single- and three-phase patterns, were studied. However, the modulation index range does not change significantly and remains within a region between 0.7 and 1 p.u. In addition to the numerical techniques, the modulation strategies were also developed to decrease the higher-order harmonics of the converter. For example, in [128], the combined switching strategy for the matrix converter was proposed, in which some of the harmonics of the input and output currents and the output voltage near the fundamental can be eliminated. A new active harmonic suppression technique was recently introduced to the line frequency method aimed at eliminating the higher-order of harmonics by creating the opposite of the harmonics to cancel them [129], [130]. However, the disadvantage is in using a high switching frequency to eliminate higher-order harmonics. Other methods have also been reported, including one where the harmonic elimination is combined with

a programmed method [131], and where multilevel pulse width modulation (PWM) defined by the well-known multicarrier phase-shifted PWM was proposed in [132] and [133]. The modulation index in this algorithm states the distribution of the switching angles, and then the problem of PWM harmonic elimination is applied to a particular operating point aiming to obtain the optimum position of these switching transitions that offer elimination to a selected order of harmonics. A generalized formulation for multi-level PWM converters with the nonequal dc source was also reported in [134].

All of these studies in addition to many others have merit because they improve the output voltage waveform. However, some of the modifications need to be implemented offline and some others would be applicable in a specific range of modulation index or with a specific switching technique. All of these methods were successful in reducing the harmonic distortion; however, some need a sensor installed inside the drive, while others need a revision for the machine or even require the machine to be dismantled, which is costly. Moreover, utilizing the drive's current in the feedback loop and generating the error signal would not be helpful when an unbalanced voltage occurs in the system. The unbalanced voltage causes the frequency response of the current to have inter-harmonics, which are not easily recognizable from the specific inter-harmonics of the control algorithms [135], [136].

The frequency response of the stray electromagnetic fields demonstrates the main harmonics orders and inter-harmonics. These inter-harmonics and disruptive harmonics decrease the power quality and cause derating of the drives. Moreover, the electromagnetic interference (EMI) of the drive would infect other adjacent components.

By monitoring these fields and utilizing them in designing the controller, the electromagnetic signature that results from the stray field could be reduced and the overall efficiency will be improved. In this chapter, a method to reduce stray field generated by a certain harmonic component is proposed. The idea is to use the radiated electromagnetic field as feedback input for the drive controller to inject negative components that cancel unwanted a stray field. The proposed method can be implemented online without a need to revise the construction of the drive. Unlike the passive filters method that reduces the radiated field from the distribution network only, the proposed method reduces the radiated field from the electric machine itself.

11.2 Harmonic Reductions of Electric Drives

There are several basic methods for reducing harmonic voltage and current distortion from nonlinear distribution loads, such as adjustable frequency drives. Prior to discussing the proposed method, the previous and existing methods are reviewed.

11.2.1 Hardware Solutions (Filters):

The adjustable frequency drive can be connected to the motor without any additional elements to control the speed. The advantage of this is low cost, ease of packaging, selling and applying; however, the disadvantage is a high level of harmonic current and voltage distortion. Many filter-based components, such as reactors, dc chokes, harmonic shunt filters, and broadband filters, were utilized. The advantage of some of these methods is low cost, providing increased input protection for the drive, flexibility in the range of impedance and being able to provide a moderate reduction in voltage and current harmonics [137]. The disadvantage of some of these methods is the requirement to be

mounted separately, as well as they may not be able to reduce the harmonic level below the IEEE 519 guidelines. Moreover, the 12 and 18 pulse converters were also utilized, which show a great reduction of harmonics of up to 85%. However, the impedance matching of phase-shifted sources is critical to the performance and the transformer often requires separate mounting. A filter based solution can reduce the stray field emitted from the distribution network connected to a high current drive system by preventing the high harmonic order from propagating to the network. However, the filter will not improve the radiated stray field from the machine. High harmonic orders and inter-harmonic will exist in the machine stray field even with the filter installed.

11.2.2 PWM Modifications:

In addition to the hardware solution, several PWM methods have been developed in order to reduce the harmonic content by controlling the drive without adding additional components. Selective harmonic elimination solves the transcendental equations characterizing harmonics, so that appropriate switching angles are computed for the elimination of specific harmonics at the output [138], [139]. These methods can provide a lower harmonic content, but the solution of these equations requires huge computation time; hence, online implementation is difficult. Switching angles are calculated offline [127], [140], or the equations are linearized before they are solved [141], [142], or an approximate solution is sought where the topology permits it [143]. Other strategies embrace modification of the carrier signal [144], [145] or the reference sine wave [146]. All of them are open-loop control schemes that assume an absolutely constant dc supply (i.e., all the harmonics produced into the grid by an inductive supply area unit are

ignored) and disregard the prevailing harmonic content of the grid voltage or the distortion caused by the load. In simple terms, they try to scale back the harmonics created by the PWM itself instead of improving the emitted stray field.

The proposed method is actually based on the modification of PWM methods through observing the magnetic stray field of the machine, not the converter. However, the converter would affect the stray fields of the machine. The behavior of the stray magnetic field of the drive is explained in the following section.

11.3 Harmonic Behaviors of Stray Fields

The stray field waveform may be characterized by a series of sinusoidal components at harmonic frequencies and sinusoidal components between the main orders of harmonics. In this section, the harmonic and inter-harmonic of the field that strayed from a drive connected to the electric motor are studied. The schematic of the proposed converter connected to the machine is shown in Figure 11.1. The common feature of such a double energy conversion system is that it contains an AC–DC rectifier and a DC–AC inverter.

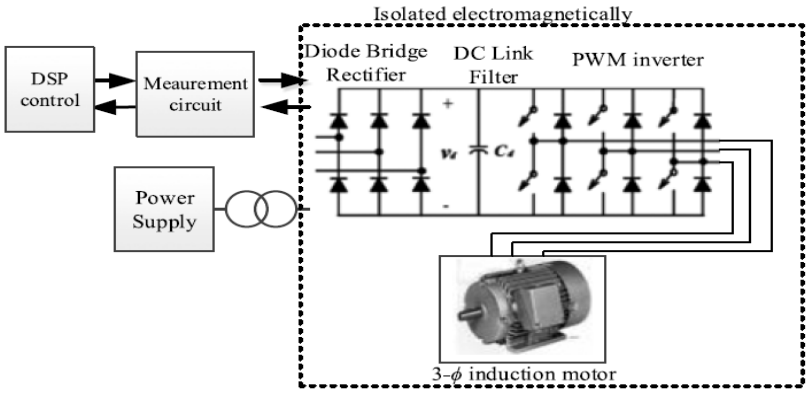


Figure 11.1: Schematic of the test setup (PWM VSI drive)

The rectifier and inverter are coupled through a dc-link filter. If the reactor or the capacitor has an infinite value, there will be no ripples on the dc side, and consequently, the ideal rectifier will only generate the characteristic harmonics ($fh-R$)

$$fh-R = (kn \pm 1)f \tag{11.1}$$

where k is the pulse number of the rectifier, n is an integer, and f is the power frequency. However, the reactor or the capacitor values are finite in practice and the ripples at the dc side are inevitable. As a consequence of not having a flat DC-link current, its AC side will be modulated by the dc ripple and the inter-harmonics could be produced. For example, for a six-pulse rectifier, based on equation (11.1), its characteristic frequencies are the 1st, 5th, 7th, 11th, 13th, and so on, in terms of harmonic orders. However, if the dc side has a ripple of, for example, 165 Hz, the ac-side current will be modulated as (1st, 5th, 7th, 11th, 13th . . .) $\pm$165 Hz. These are inter-harmonic components.

Contrasting current source converters, voltage source converters needed more complex formulas to determine the dc ripple generated by the inverter [2]. In the case of the sinusoidal PWM modulation technique (SPWM), the harmonic frequencies generated by the inverter are evaluated as follows:

$$f_{\text{ripple}}(mf,\ i,\ j) = |mf\, i \pm j| \cdot f_{\text{output}} \tag{11.2}$$

where mf is the modulation ratio with i and j as the integers depending on the modulation ratio. The $f$output is the output frequency. The dependence of mf is related to the switching strategy adopted. When mf is not triple and odd, by having even or odd i, the j

would be even or odd, respectively. On the other hand, while *mf* is triple and odd, by having even or odd *i*, the *j* would be even triple or odd triple, respectively. However, if *mf* is even, *j* can be even or odd, and triple for triple*mf* [147]. Note that the frequencies generated by inverters revealed in equation (11.2) will modulate with the rectifier's characteristic harmonic of equation (11.1) and subsequently the supply-side frequencies will be generated

$$f\text{ss} = fh - R \pm f\text{ripple} \tag{3}$$

The supply-side frequencies *f*ss are actually the interharmonics of the power frequency as long as *f*ripple is not synchronous with *f*. As discussed, the harmonics and inter-harmonics appear in the frequency response of the radiated magnetic fields.

11.4 Control and Optimization Procedure

The electromagnetic reduction strategy is based on the harmonics and inter-harmonics of the converter connected to the machine since the main harmonic contents are originating from the converter switching and affecting the performance of the machine. Based on the discussion in previouse section, the control algorithm is designed and discussed here in this section. The structure of the proposed controller is composed of three blocks: a) sensor and conditioner; b) spectrum computation; and c) main control. These blocks are shown in Figure 11.2.

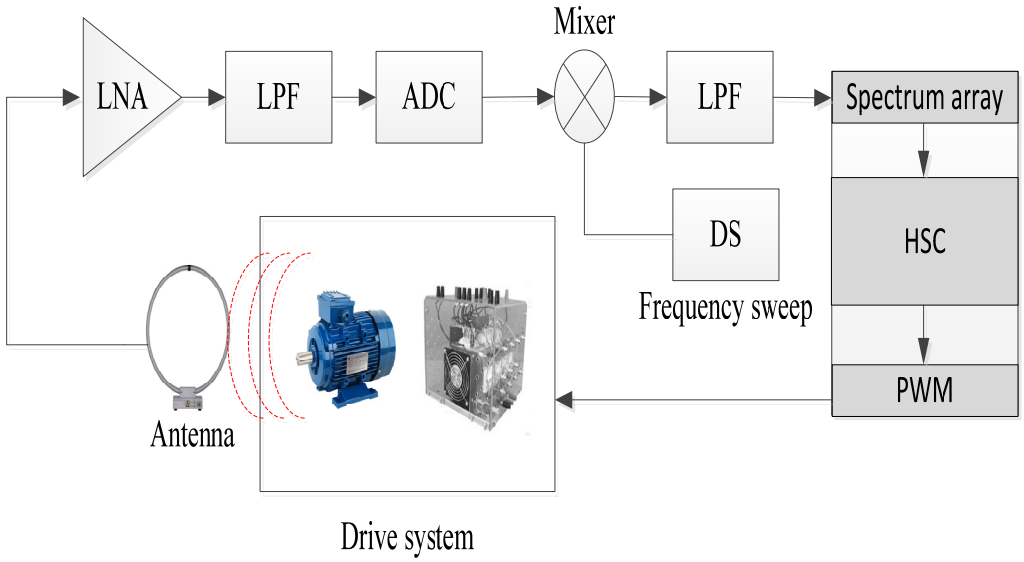


Figure 11.2: The procedure of the controller

a) Sensor and Conditioner Block

The magnetic fields of the drive are measured using the magnetic coil antenna. (The details of the antenna and other components are mentioned in the next section.) The measured signal first buffered and amplified using a low noise amplifier. The amplified signal is then passed through a low-pass filter (LPF) before the analog to digital conversion stage.

b) Spectrum Computation Block

The spectrum calculation is based on the heterodyne receiver. Heterodyning is a radio signal processing technique in which new frequencies are created by combining or mixing two frequencies[147]. Heterodyning is useful for frequency shifting signals into a new frequency range and is also involved in the processes of modulation and demodulation. The two frequencies are combined in a nonlinear signal processing device,

such as a vacuum tube, transistor, or diode, usually called a mixer. The most important and widely used application of the heterodyne technique is in the superheterodyne receiver. In this circuit, the incoming radio frequency signal from the antenna is mixed with a signal from a local oscillator and converted by the heterodyne technique to a fixed frequency signal called the intermediate frequency (IF). The resulting IF signal is filtered by a narrow band LPF to isolate the desired frequency spectrum. The output magnetic fields spectrum would be transmitted to the main controller. This receiver is composed of three basic components: 1) variable sinusoidal wave generator, which is programmed through a direct digital synthesizer (DS); 2) LPF; and 3) a multiplier, as shown in Figure 11.2.

1) Variable Sinusoidal Wave Generator: In this system, the heterodyne receiver multiplies the amplified signals with two quadrature sinusoidal signals generated by a direct digital synthesizer (DS), which generates a variable frequency sinusoidal signal. The DS is a type of frequency synthesizer used for creating arbitrary waveforms from a single, fixed-frequency reference clock. The heterodyne receiver was implemented digitally inside the microprocessor. The DS was implemented using a digital oscillator for increasing the oscillator stability and simplifying the frequency control. The modified coupled form of the oscillator shown in Figure 11.3 is used to produce a high purity sinusoidal wave while using low processor resources [148]. Only two multiplies and two summation operations need to be performed for each sample output. The oscillator frequency can be changed dynamically by changing ε, where $\varepsilon = \omega/\pi$. The oscillator outputs $x[n]$, $y[n]$ represent two near quadrature sinusoidal signals, being off by one-half

sample. The quadrature sinusoidal outputs are digitally multiplied by captured signals from the antenna after amplification.

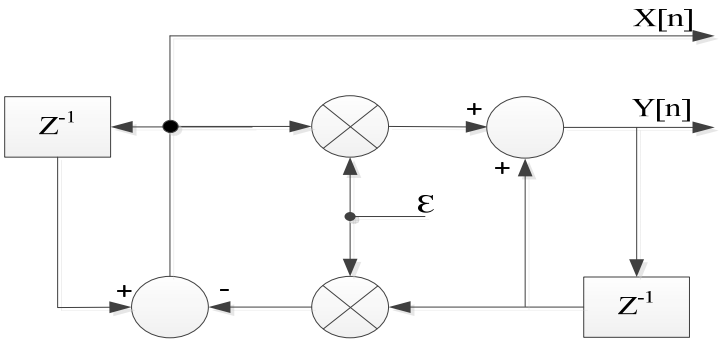


Figure 11.3: Digital oscillator scheme

2) LPF and Multiplier: A narrow-band low-pass FIR filter was used to isolate the spectrum magnitude, as shown in Figure 11.4. The phase angle of the signal can be obtained with respect to the oscillator angle by calculating tan−1 (*Xs* [*n*]*/Ys* [*n*]). Different harmonic orders were captured by sweeping the oscillator frequency. Also, the harmonic order and magnitude were captured and stored in a matrix to be used by the harmonic suppression block. The implementation for the spectrum computation was done under the control of a 32-bit reduced instruction set computing (RISC) processor. RISC is a CPU design strategy based on the insight that simplified (as opposed to complex) instructions can provide higher performance if this simplicity enables much faster execution of each instruction [149]. ARM (Advanced RISC Machines) cortex M4 processor with 210 DMIPS (dhrystone million instructions per second) and DSP extension was chosen for the implementation. Fast instruction execution, hardware multiplier, and DSP instruction make it possible to run the spectrum analysis and harmonic compensation algorithm, the 12 bit analog to digital with speed up to 2.4 MSPS

(Mega Samples Per Second) and direct memory access allow capturing signals with a high accuracy and sampling rate. The harmonic search and compensation algorithm were built using a finite-state machine, which simplifies task management without using a real-time operating system and reducing the execution overhead.

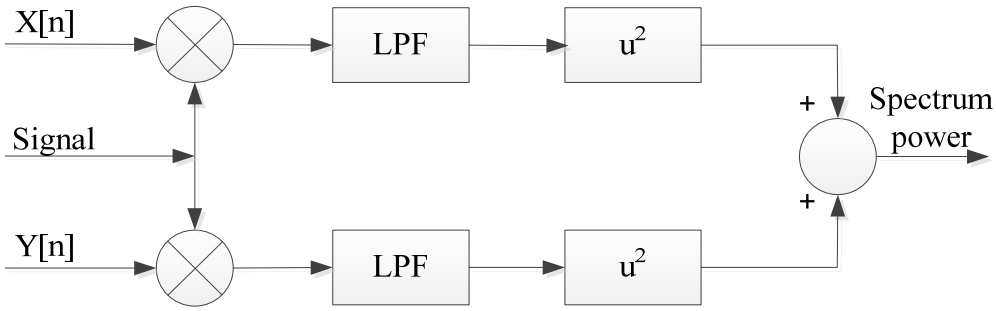


Figure 11.4: Spectrum analysis procedure

c) Main Control Block

A fast serial communication link was used to transfer the spectrum from ARM cortex M4 processor to dSpace 1104 embedded controller. The dSpace embedded controller is used to implement the real-time control of the power electronics converter and the Harmonics Suppression Controller (HSC). After transmitting the magnetic field spectrum to the main controller, the measured fields would be categorized into the main and sub-harmonics. Each harmonic would be compared with the desired predefined harmonic magnitude and the error signal is passed to the harmonics suppression controller HSC.

The main function of the HSC is to generate modulated signals that will cancel the unwanted harmonic spectrum by finding the correct magnitude and phase angle for each frequency. These modulated signals are then added to the sinusoidal modulated signal used in a PWM controller. This technique has an advantage over the classical method of

decreasing unwanted harmonics by increasing the frequency ratio. Increasing the frequency ratio can reduce the main harmonics results from switching activity on the inverter only, whereas the proposed technique can reduce the main and inter-harmonic results from the inverter and the machine itself. Moreover, the harmonic suppression process is selective and does not affect the average switching frequency. The online feedback for the HSC makes the system adaptive to different environments and machine conditions. Furthermore, the operator can select to suppress specific harmonics that cause interference with other systems. The details of methodology, as well as the modulation algorithms, are described in the next section.

11.5 Harmonic Suppression, Discussion, and Results

The procedure of suppression is implemented in two well-known switching algorithms, SPWM) and SVPWM techniques with comprehensive comparison. The summary of the aforementioned switching algorithms and the optimization in their design is explained in the following section [150]–[152].

11.5.1 Sinusoidal PWM

The sinusoidal PWM is a type of “carrier-based” PWM. Carrier-based PWM uses predefined modulation signals to determine the output voltages. In sinusoidal PWM, the modulation signal is sinusoidal with the peak of the modulating signal always less than the peak of the carrier signal. The details of this well-known method are illustrated in [150]. There are two significant drawbacks with sinusoidal PWM. First, the converter with this modulation generates a less line-line output voltage with the same amplitude of the line supply. The other disadvantage, which is more related to the electromagnetic

signature, is the short pulses. If the output is to be truly sinusoidal PWM, it is important to include very small pulses when the peak modulation signal is close to the peak carrier voltage. These small pulses can contribute significantly to inverter losses, while not significantly affecting the output voltage. In addition, small pulses may be impractical due to the time required to switch one device off and another device on [151]. Hence, they create high-order harmonics. However, these harmonics may not be seen in the output voltage or current; they generate low- and high-order harmonics of the stray field [147]. The harmonic orders of magnetic stray fields of an induction machine drive connected to the converter and controlled through SPWM are shown in Figure 11.5.

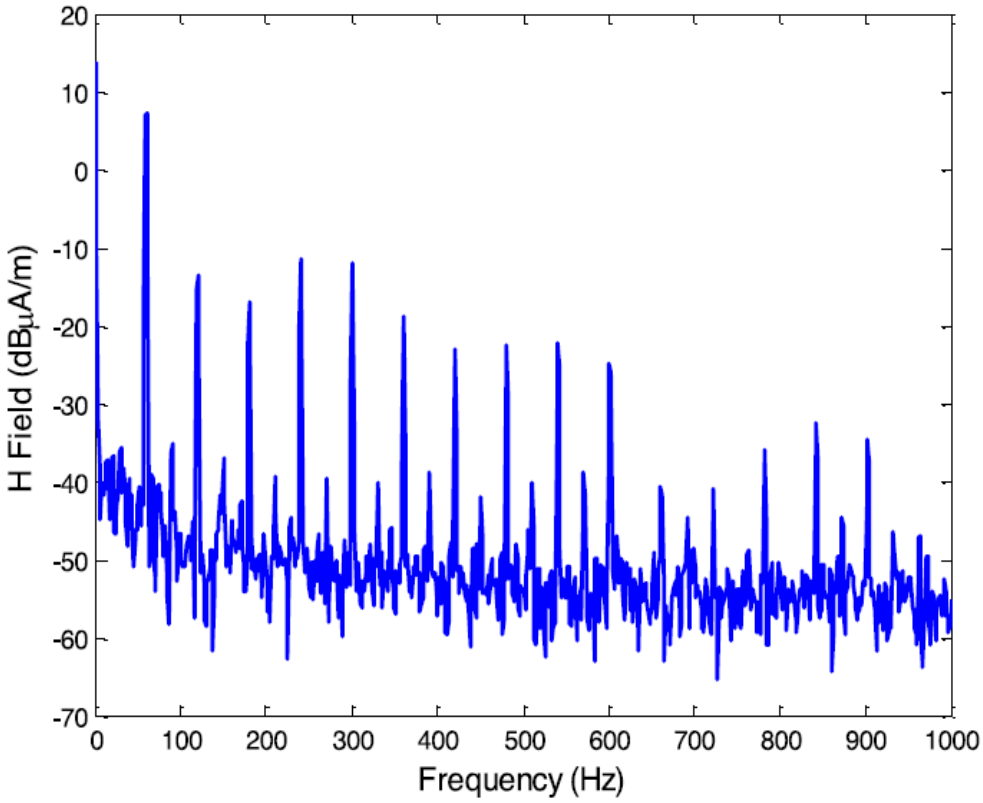


Figure 11.5: Magnetic field intensity (H) of the induction motor connected to the drive using the SPWM technique

In order to decrease the harmonic orders shown in Figure 11.5, two methods are implemented in this paper: manual and automatic techniques. Both methods were applied in real-time operation. The setup and the details of the components are reflected in Table 1 and Figure 11.6.

Table 11-1: Details of the Components in the Testbed Setup

Component	**Characteristics**
Multifunctional converter	Six IGBT switches, I:80 A, V_{CES}: 1200V.
Induction motor	7.5 HP, 208 V, 1765 r/min, PF: 0.82, 60 Hz, EEF: 89.5%
Digital controller	dS1104 R&D Controller Board and Connector Panel
RISC processor	STM32F407, 168 MHz, CPU, 192 KB SRAM
EMI receiver/spectrum analyzer*	Coverage between 1 Hz and 3 GHz, absolute amplitude accuracy: +/- 0.5 dB to 3 GHz, displayed average noise level: - 142 dB.m/Hz at 26.5 GHz - 155 dB.m/Hz at 2 GHz and - 150 dB.m/Hz at 10 kHz
Magnetic coil antenna	Coverage between 20 Hz and 500 kHz, 36 turns of 7-41 Litz wire shielded with 10 Ω resistance and 340 μH inductance.

*Measurement components are MIL-STD 461F standard compliant.

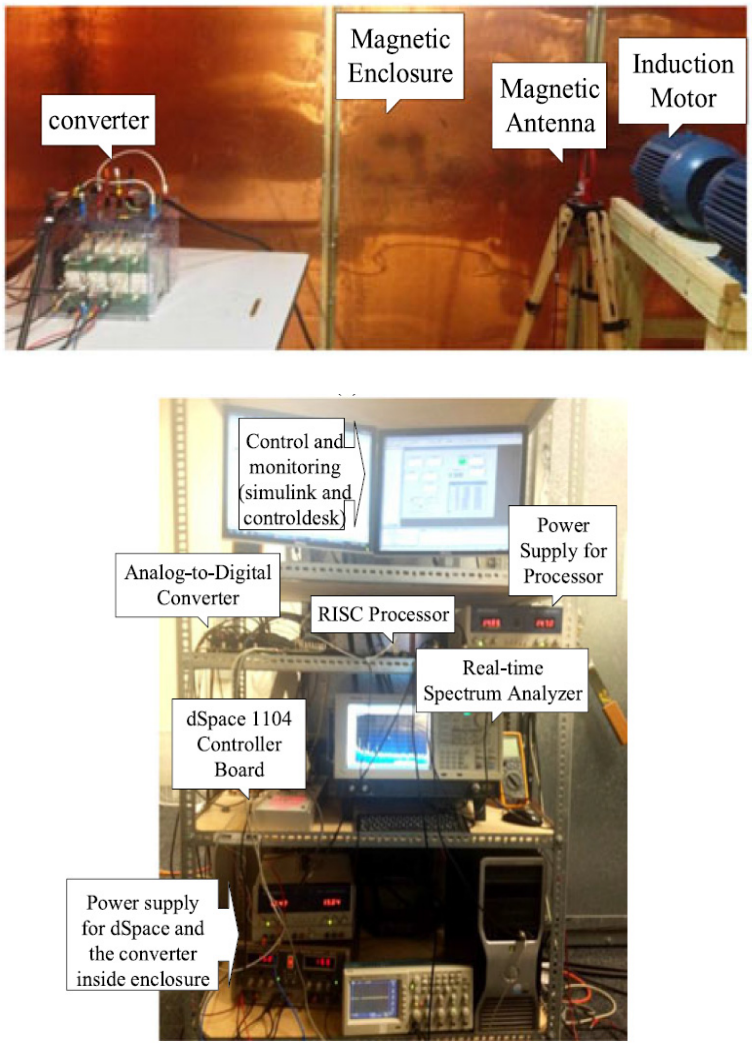


Figure 11.6: (a) Setup inside the enclosure (the converter and the motor) and (b) control and monitoring setup. Note that the antenna is located 12 in away from the center of the machine (~3 inch from the cage)

11.5.2 SPWM Harmonics Manual Suppression

In the manual technique, the proportional amplitude of the most harmful harmonics is injected into the control block to decrease the overall amplitude. The amplitude and phase offset of the harmonic suppression block is set initially in Simulink and connected to the dSpace 1104 digital controller interface, which can be controlled in real time. The switching algorithm would be modified accordingly and the signal was transferred

through the dSpace to the converter. In order to suppress the noises of the signal processing components and all other elements, the machine and inverter were located inside an enclosure, which was isolated electromagnetically, as shown in Figure 11.6. The procedure of signal processing used in the test was mentioned in the previous section. The block diagram of the control block for the manual suppression is shown in Figure 11.7. The control of frequency is used for setting the desired harmonic to be suppressed. Moreover, the amplitude and the phase offset can be adjusted for setting the harmonics to have the most appropriate suppression. Three critical harmonics of the machine, including 2nd, 4th, and 5th harmonics, were selected to be suppressed manually. Therefore, the frequency of the suppression was set based on their harmonic order and the amplitude and phase offset was adjusted in real-time in the control desk interface. The even harmonics and main odd harmonics (5th, 7th, 11th, . . .) are selected as the harmful harmonics, which are originated due to the presence of a power electronics component in the drive. Figure 11.8 shows that by adjusting the HSC to suppress the second harmonic, the second harmonic of the stray field of the machine decreases from −15 to −25 dB·μA/m. The block was designed to decrease the second harmonic, but some other higher harmonics, such as eleventh and thirteenth, which are harmful harmonics, are also reduced. The amplitude of the block for suppressing the second harmonic was set to 3 and the phase angle was set to 0.7 rad. The total harmonic distortion (THD) up to the 10th harmonic order for the cases without HSC and with HSC is 0.63% and 0.37%, respectively. Accordingly, the study on the fourth harmonic and fifth harmonic of the motor are also demonstrated in Figure 11.9 and Figure 11.10, respectively. Similar to the second harmonic case, the HSC also performed substantially

for the fourth and fifth harmonics. Note that the changing of the amplitude and phase angle of the suppression block is real time.

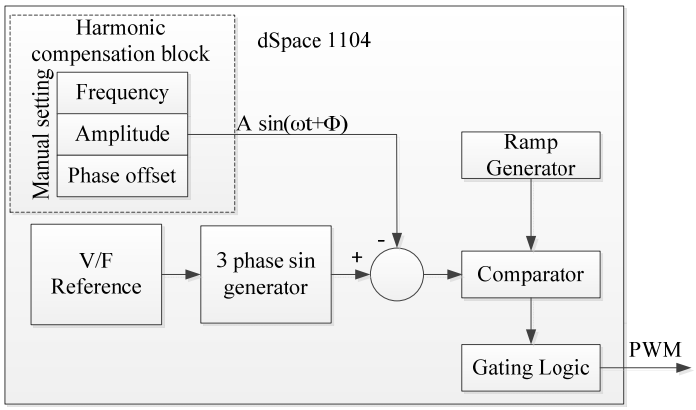


Figure 11.7: Block diagram of the sinusoidal PWM with harmonic compensation block

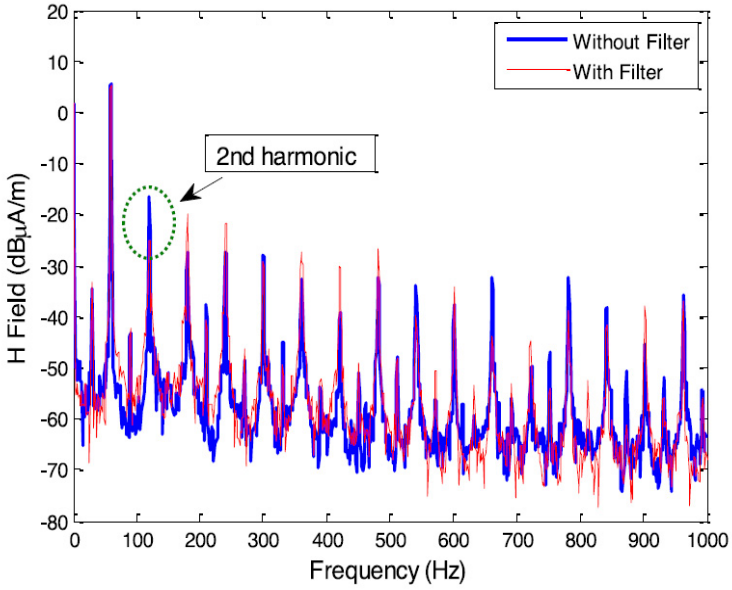


Figure 11.8: Magnetic stray field intensity (H) of induction motor using SPWM with and without HSC for second harmonic suppression

The manual method is appropriate for reducing the level of harmonics to a specific level. The THD for the cases without HSC and with HSC is 0.6% and 0.31%, respectively, for Figure 11.9, and 0.63% and 0.25%, respectively, for Figure 11.10.

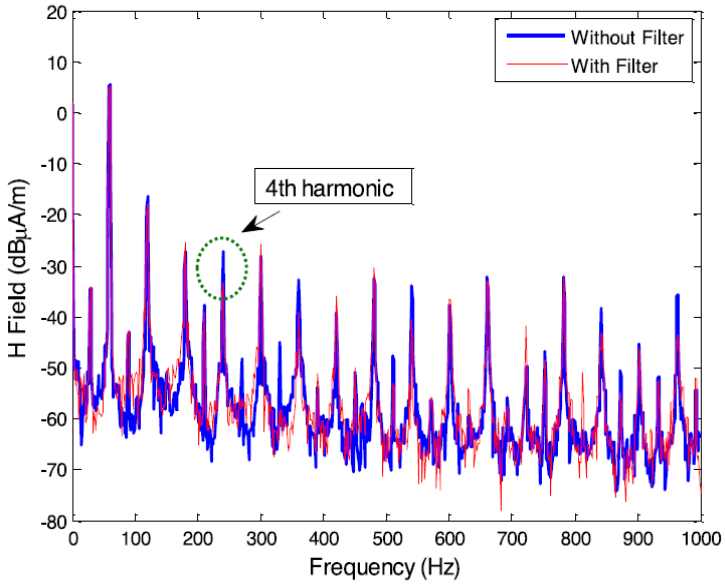


Figure 11.9: Magnetic stray field intensity (H) of induction motor using SPWM with and without HSC for fourth harmonic suppression

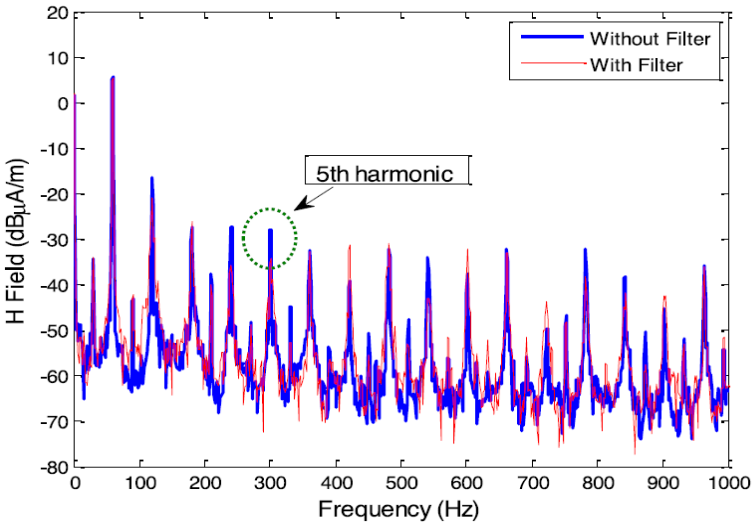


Figure 11.10: Magnetic stray field intensity (H) of induction motor using SPWM with and without HSC for fifth harmonic suppression

11.5.3 SPWM Harmonic Automatic Suppression

In the automatic suppression, the harmonic contents of the drive are being captured by the antenna and sent to the processor through ADC. Based on the procedure of the

signal processing, shown in Figure 11.2 and Figure 11.6, the existing harmonic content was compared with the actual one and subsequently the appropriate switching signals to the switches to reduce the level of the proposed harmonic(s). The difference of this controller shown in Figure 11.11 as compared to the manual one (see Figure 11.7) is replacing the manual control of the amplitude and the phase shift of the harmonic compensation block by the tracking algorithm. The HSC in Figure 11.11 is based on a tracking algorithm. The tracking algorithm is performed using a state machine with three states, as shown in Figure 11.12. The *Init state* is for initialization of the amplitude of the respective harmonics to be canceled. The next state is the *Phase_tracking,* where depending on the spectrum error, the phase increases or decreases. The spectrum error is defined as follows:

$$\text{Error}\,(t) = \text{Spectrum}\,(t) - \text{Spectrum}\,(t-1) \tag{4}$$

where Spectrum (t) is the average of 20 samples of spectrum and Spectrum (t – 1) is the previous average of the same spectrum. The rules for the phase tracking are as follows: if Error is positive, the phase increases and if Error is negative, the phase decreases. Once the phase tracking algorithm has reached the minimum spectrum at the harmonic frequency in analysis defined as a threshold, then next state is *Amplitude_tracking*. The *Amplitude_tracking* state follows a similar rule as *Phase tracking* algorithm. If the error is positive, the amplitude increases and if the error is negative, the amplitude decreases. Finally, the suppression was implemented in real time and the result was obtained (see Figure 11.13). Comparing this figure with the manual test in Figure 11.9, the suppression was about 50% more. Moreover, some other even

harmonic orders, such as sixth, were reduced. The optimum amplitude that the system showed was 18 V and the phase angle was 0.85 rad. The THDs for the cases without HSC and with HSC for Figure 11.13 are 0.51% and 0.44%, respectively.

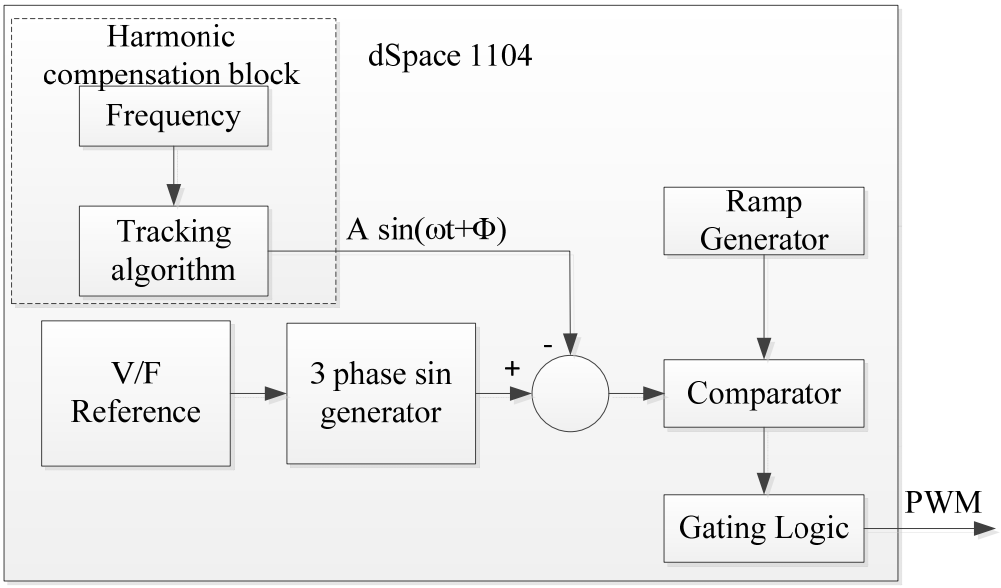


Figure 11.11: Automatic harmonic suppression block diagram

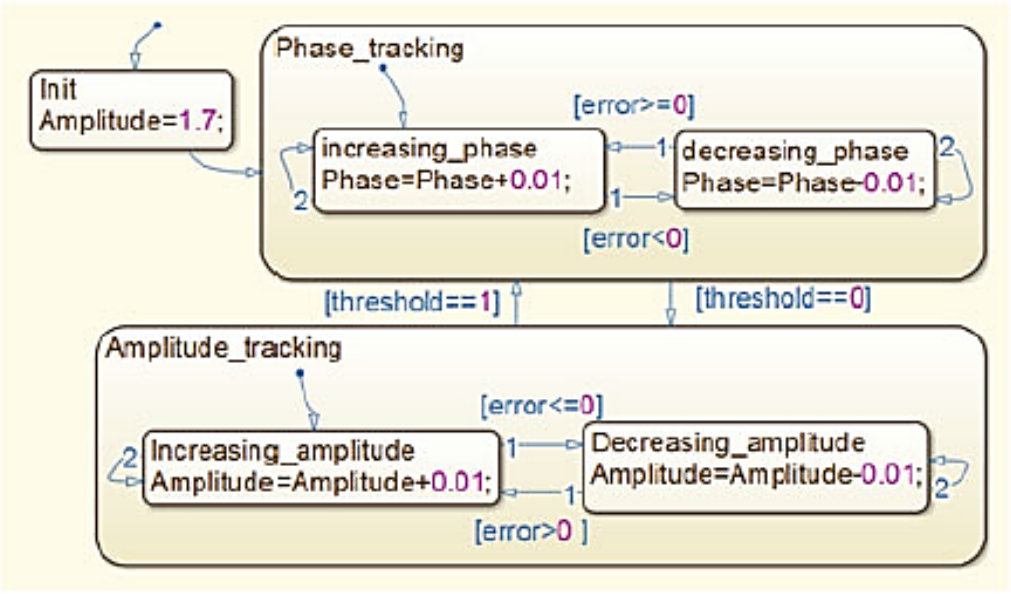


Figure 11.12: State machine tracking algorithm

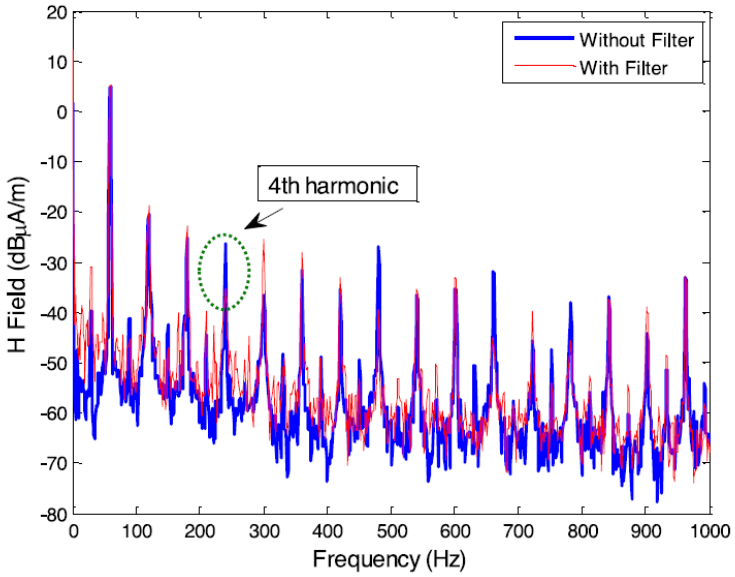


Figure 11.13: Magnetic stray field intensity (H) of induction motor using SPWM with and without HSC for fourth harmonic suppression in automatic mode

11.5.4 SVPWM

As one of most promising modulation technologies in three phase systems, SVPWM for a three-level converter has an advantage over sinusoidal PWM in voltage utility. The SVPWM output voltage is 15% higher than that of sinusoidal PWM [35]. Therefore, this method, as one of the main modulation technologies, was also used in this research for both manual and automatic suppressions.

11.5.5 SVPWM Harmonic Manual Suppression

The manual suppression procedure is similar to the SPWM case, except the changes in the modulation method, which is shown in

Figure 11.14. The fourth and fifth harmonic orders of the motor at 240 and 300 Hz, similar to the previous case, are selected to be suppressed. The magnetic stray field of the

induction motor at the same distance in these two cases is shown in Figure 11.15 and Figure 11.16. As Figure 11.15 and Figure 11.16 illustrate, there is good suppression at the intended harmonic orders, more than 10 dB·μA/m. Furthermore, the other higher harmonic orders are also suppressed. The amplitude of the HSC block for the fourth and fifth harmonic suppression was 19 and 16.9Vand the phase offset was 0.12 and 0.411 rad, respectively. The THDs for the cases without HSC and with HSC are 2.02% and 1.55%, respectively, for Figure 11.15, and 2.02% and 0.16%, respectively, for Figure 11.16. In addition to the singular harmonic suppression, multiple harmonic suppression can also be implemented by adding a multiple harmonic suppression (HSC) block. For instance, the suppression of simultaneous fourth and fifth harmonic orders was also implemented. The result is demonstrated in Figure 11.17.

Both intended harmonic orders are suppressed considerably. Moreover, many other harmonic orders in the neighborhood are also suppressed. In this case, there are two amplitudes and two phase offsets. The amplitude and phase shift of the HSC block for the fourth harmonic suppression was 19 and –0.12 rad and for the fifth harmonic suppression was 4 V and 0.08 rad. The THDs for the cases without HSC and with HSC for Figure 11.17 are 2.01% and 0.73%, respectively. Note that since the computation would increase by adding HSC blocks, the processor would stop working or delay in the answer if the number of blocks went over 2 by using the mentioned processor.

11.5.6 SVPM harmonic Automatic Suppression

The procedure of the automatic suppression in SVPWM is the same as the SPWM case. The harmonic compensation block of

Figure 11.14 was modified as it was modified in the SPWM case in Figure 11.11. The amplitude and the phase angle obtained from the real-time test were 17.5 V and 0.1 rad. The THDs for the cases without HSC and with HSC for Figure 11.18 are 2.01% and 0.9%, respectively. Comparing Figure 11.18 with Figure 11.15, the fourth harmonic was decreased to about –30 dB·μA/m, which was about 10 dB·μA/m better than the manual case.

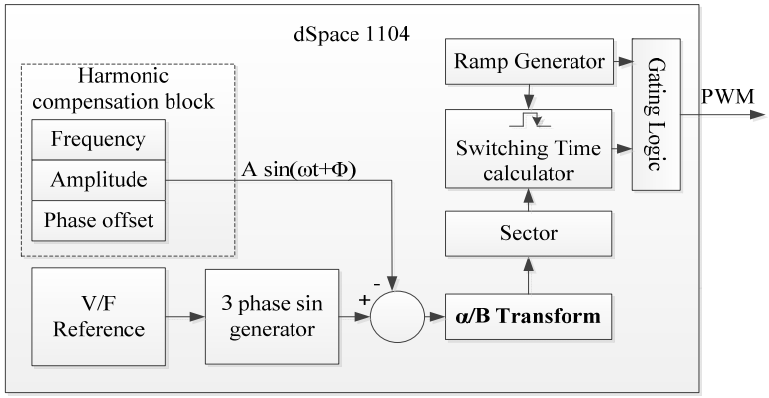


Figure 11.14: Block diagram of the SVPWM with harmonic compensation block

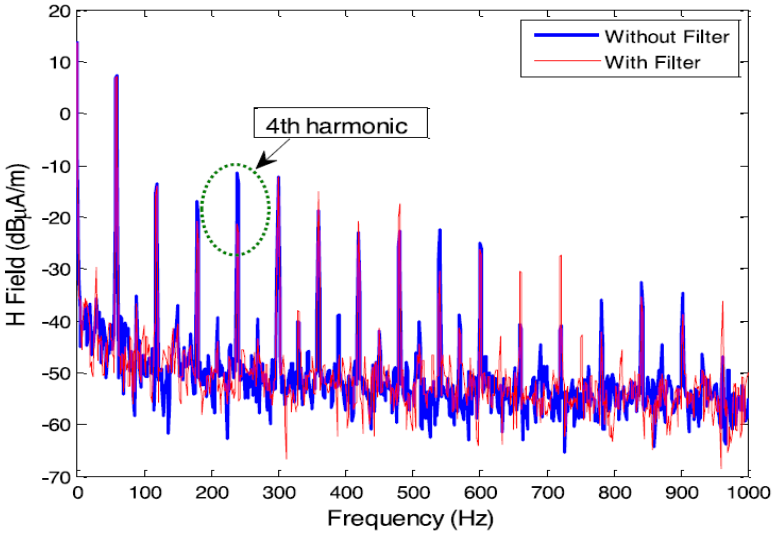


Figure 11.15: Magnetic stray field intensity (H) of induction motor using SVPWM with and without HSC for fourth harmonic suppression

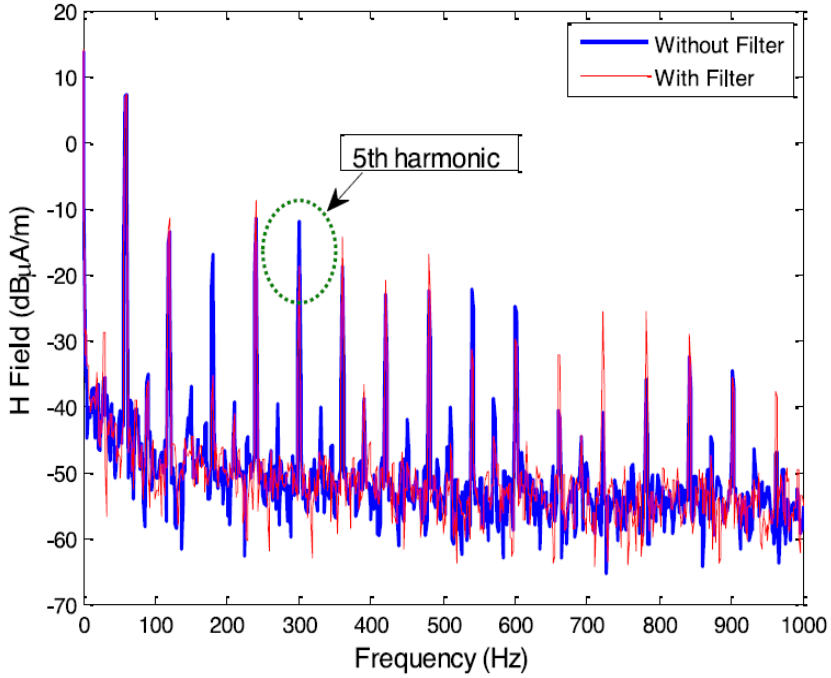


Figure 11.16: Magnetic stray field intensity (H) of induction motor using SVPWM with and without HSC for fifth harmonic suppression

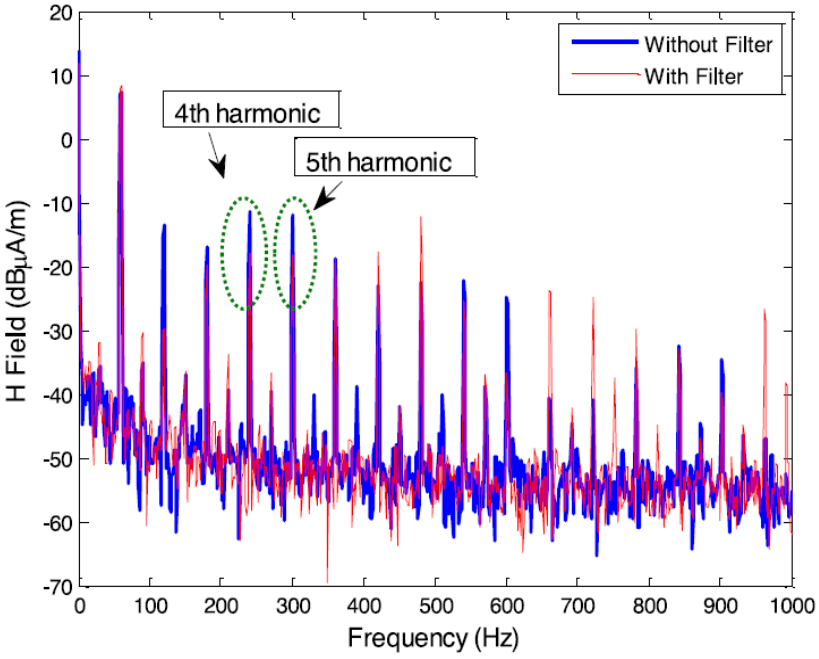


Figure 11.17: Magnetic stray field intensity (H) of induction motor using SVPWM with and without HSC for simultaneous fourth and fifth harmonic suppression

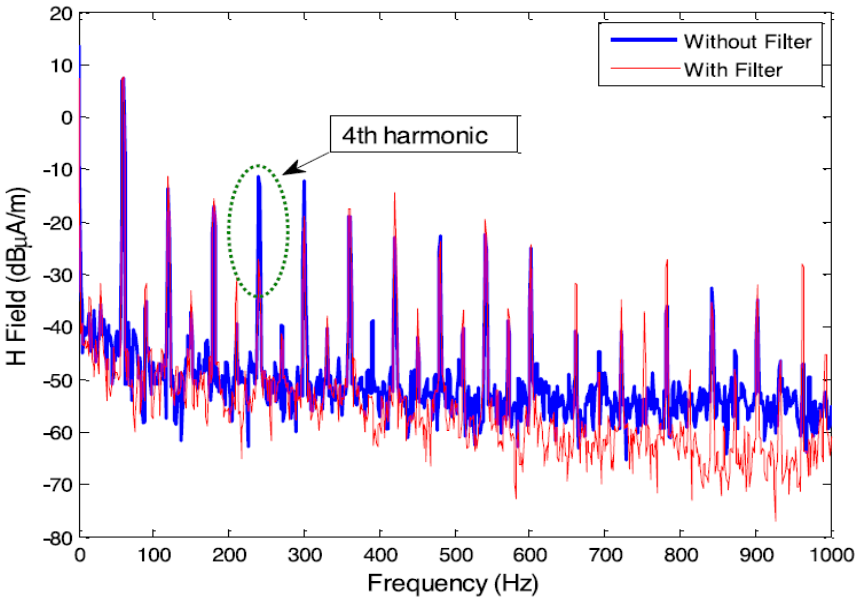


Figure 11.18: Magnetic stray field intensity (H) of induction motor using SVPWM with and without HSC for fourth harmonic suppression in automatic mode

11.6 Summary

Improving the design scheme of the switching algorithm of power electronics converter and motor drive to reduce the stray field for selected harmonic component was implemented. A modification was implemented using the magnetic field of the machine as the input to the control system. The sinusoidal and SVPWM were implemented and the harmonic suppression block was added to them. The suppression was implemented for several critical harmonic orders in two manual and automatic modes. Both modes were real time. The results show that the ripples and THD are decreased in all cases; consequently, the noise is decreased and the efficiency is increased. The results show that the control using the automatic mode had better suppression in the targeted harmonics because of changing the phase angle and amplitude in a higher range and resolution in comparison with the manual mode. The method can be used for both steady state and

transient condition; however, very fast response microcontrollers and controllers are needed for the transient cases.

The advantage of this technique is that there is no need for any sensor inside the machine or any revision for the machine. Furthermore, there is no need that the modification in design is implemented and it can also be applicable in any range of modulation indices or with any switching technique. The proposed HSC can reduce the radiated field from multiple frequency components, which reduce the electromagnetic signature and improve critical system security.

Chapter 12 IEC 61850 Security Analysis

12.1 Introduction

Substations are an essential part of the transmission and distribution system. Substation controls the power flow between transmission and distribution networks. In the smart grid, substations will play a vital role in interconnecting distributed generation located on the distribution side with the transmission network and end customers. In addition, substations are a key component in monitoring and aggregating power from microgrids.

For decades, substation automation and control were dependent on a low-speed serial communication between substation digital devices, while the connections with instrumentation and circuit breakers were made using an analog connection over copper wires. These types of control and automation networks have several drawbacks, first complex wiring makes it time-consuming and costly to install, commission and maintenance. Second, in absence of interoperability standard, vendors implemented property or standard communication protocols designed for other domains, such as a Local Operating network (LON), MODBUS, PROFIBUS, FIELDBUS and DNP. Data exchange between non-compatible protocols is made through complex protocol translators. This complexity in installation, data exchange, and maintenance arise the need for data modeling and a communication standard.

The IEC 61850 is a substation automation standard developed by the International Electrotechnical Commission (IEC) technical committee Number 57 (TC57) Working Group 10 (WG10) and IEEE [153]. The IEC 61850 is developed to ensure the

interoperability between IEDs manufactured by different Vendors, simplify installation and maintenance of the substation automation system.

The IEC 61850 replaces the copper wiring and analog connection in the substation automation systems by an Ethernet-based network. An ethernet-based communication network provides higher speed and bandwidth, which allows a faster response. Moreover, it allows free allocation of the functions. Figure 12.1 and 12.2 show a comparison between the wiring and configuration of the substation automation system with the serial data bus and IEC 61850 standard. In Figure 11.1, IEDs are connected to the Current Transformers (CTs), Voltage transformers (VTs) and switchgear using copper cables. Voltage and current measurements are transmitted as analog signals. IEDs and Human Machine interface exchange information over the low-speed serial bus (station Bus), such as PROFIBUS. Figure 12.2 shows the substation automation architecture with IEC 61850. Analog measurements from CTs, VTs, and switchgear signals are connected to the process Bus through merging units. Merging units convert analog measurements to digital data and transmit them over the high-speed Ethernet network (Process Bus). Data shared over the process bus can be shared with all IEDs connected to the bus. IEDs are communicated together and with HMI over Ethernet-based station Bus Sharing instrumentation data, such as voltage and current measurement over Ethernet network simplify the installation, reduce the wiring and allow free allocation of the functions without the need to modify the wiring.

Figure 12.3 shows the direct connection of instrumentation devices (CTs, VTs) to IEDs. In this connection scheme, the analog signal is hardwired to the IED. The IED

convert the analog signal to digital form using embedded analog to digital, then the digital data is used to perform the assigned IED function.

Relocation of the IED function requires changing of a hardwired connection. Figure 12.4 shows the connection of instrumentation devices to the process bus through merging unit. The analog signal is connected to the merging unit, which converts it to digital form and transmits it to the IEDs through Ethernet-based network process bus. IEDs receive digitized data through the Ethernet connection. Relocation of functions from IED to another doesn't require wiring modification.

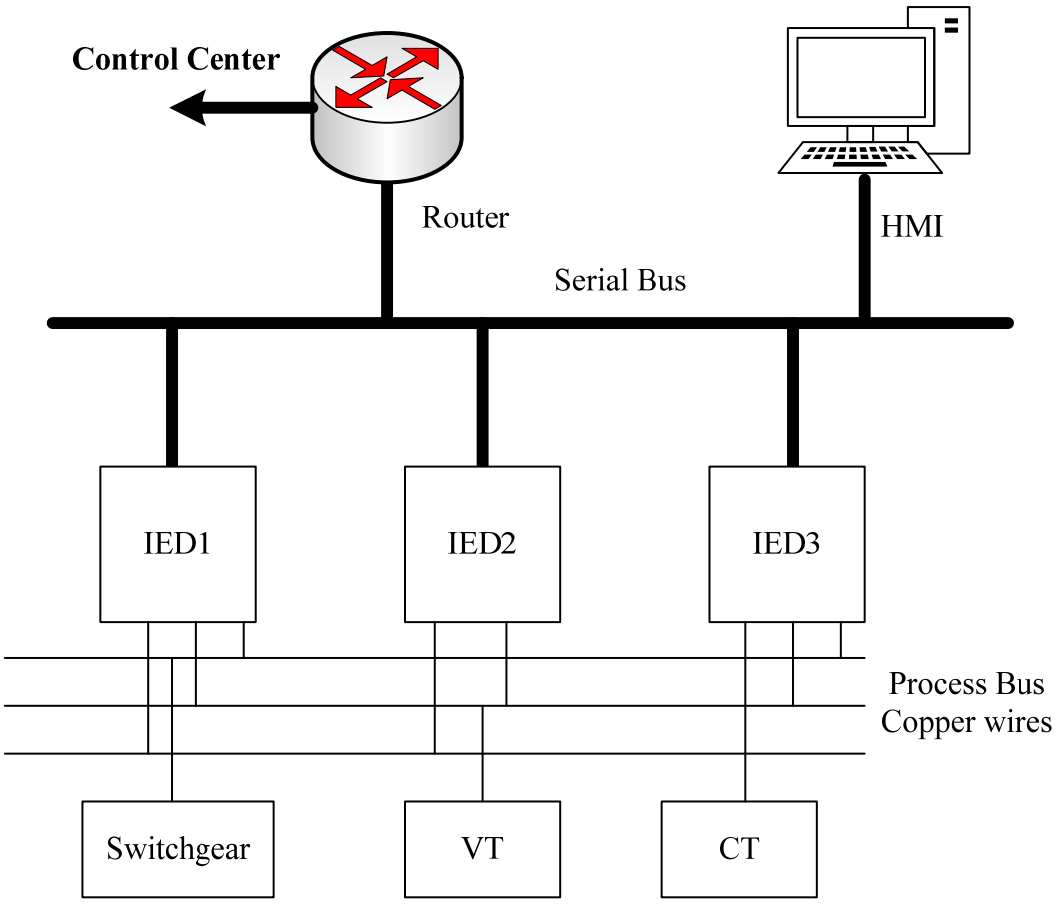


Figure 12.1: Substation automation using serial data

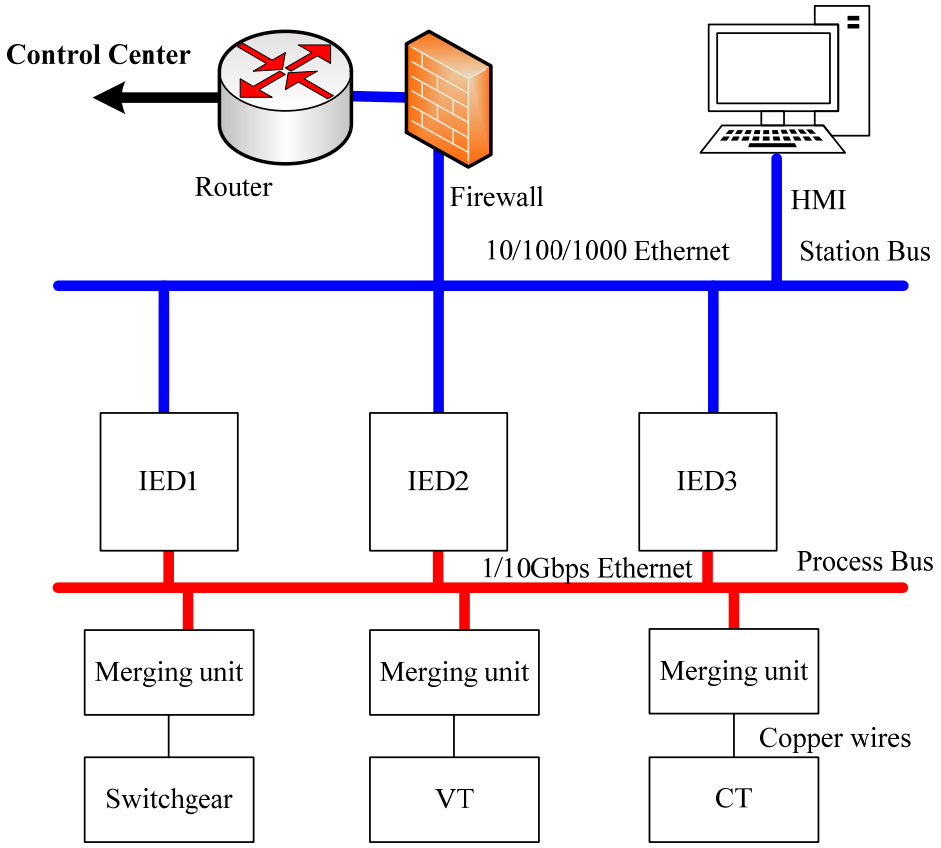


Figure 12.2: IEC 61850 substation automation.

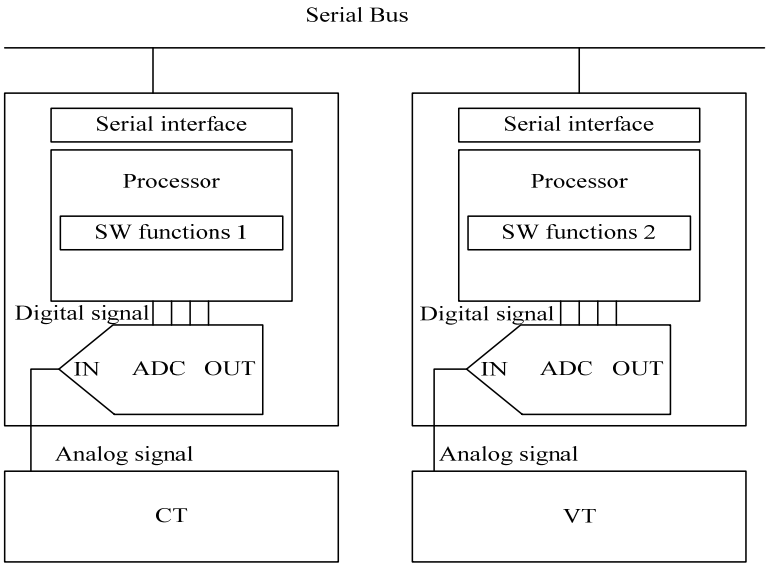


Figure 12.3: Direct connection of instrumentation devices without process Bus

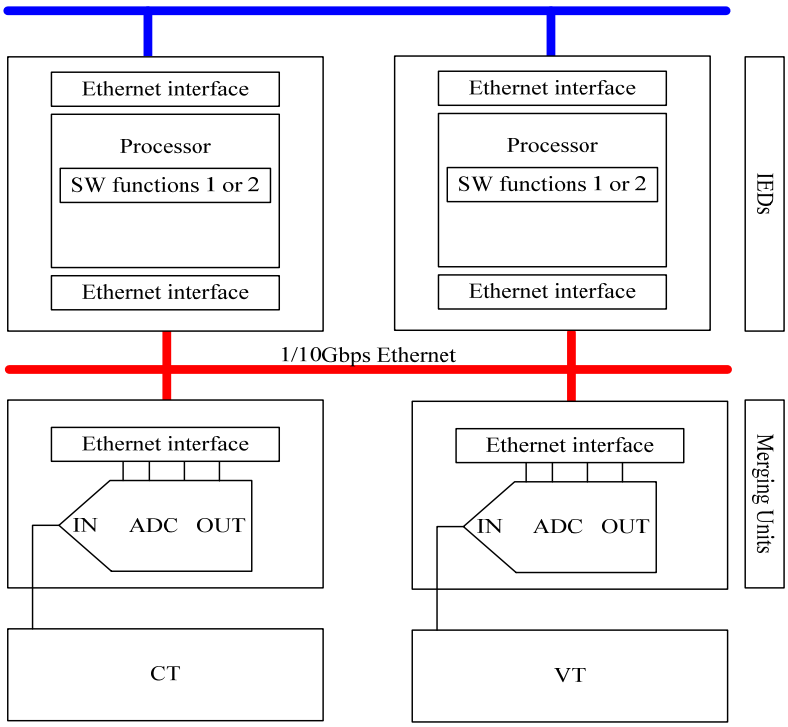


Figure 12.4: Connection of instrumentation devices with merging units and process Bus

12.2 IEC 61850 Overview

IEC 61850 defines a data model for the substation automation device to ensure data consistent across different IEDs from different vendors. The IEC 61850 Hierarchical data model start with the physical device. The Physical Device (PD) is a hardware device that connects to the network and has computation and hardware resources to run the firmware. Each PD contains one or more Logical Device (LD). The LD device consists of one or more Logical Nodes. The logical node is the smallest part of a function that exchanges data. A logical node is a data object that consists of data elements and service (Methods) related to power system function. IEC 61850 provide Abstract Communication Service Interface (ACSI) that allows the creation of data object and service independent from underlying communication protocols [153], as shown in Figure 12.5. IEC 61850-5 maps

the abstracted data model to three different protocols, Manufacturing Message Specification (MMS), Generic Object Oriented Substation Event (GOOSE) and Sampled Measured Values (SMV), as shown in Figure 12.6. The MMS is ISO 9506 standard developed originally by the International Organization for Standardization (ISO) Technical Committee 184 (TC184) for industrial automation. MMS utilizes a client-server communication scheme to provide one to one connection. The MMS messages use IP address to route the message over layer three of the OSI model. MMS protocol is used mainly for communication between IEDs. GOOSE messages are used for fast transfer of substation events such, as tripping signal [153].

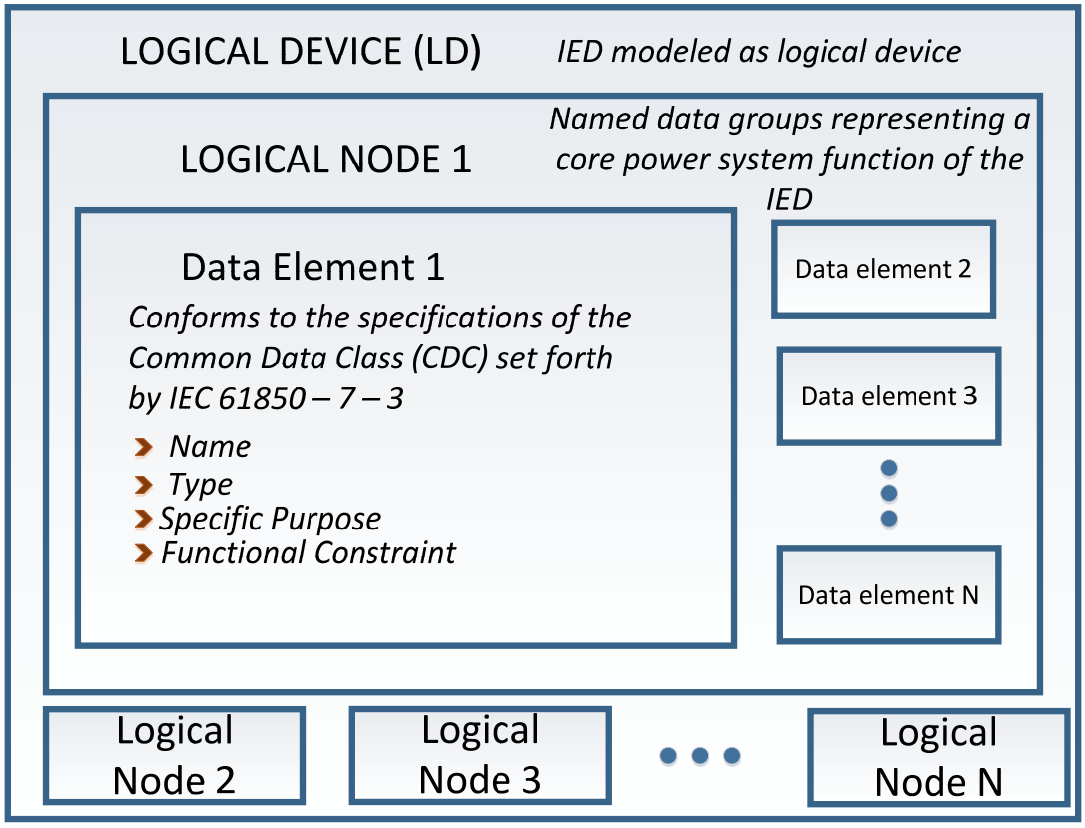


Figure 12.5: IEC 61850 data model

Since GOOSE message is used in a critical time event, a 4 ms restriction is applied for transmission. To ensure fast transmission, the data is sent over layer 2 of the OSI model. GOOSE messages are transmitted over separate VLAN with priority tag to ensure appropriate transmission priority. SMV messages are used to transfer voltage and current measurement from merging units to IEDs. Similar to GOOSE messages, SMV messages are transmitted over layer 2 with multicast MAC address.

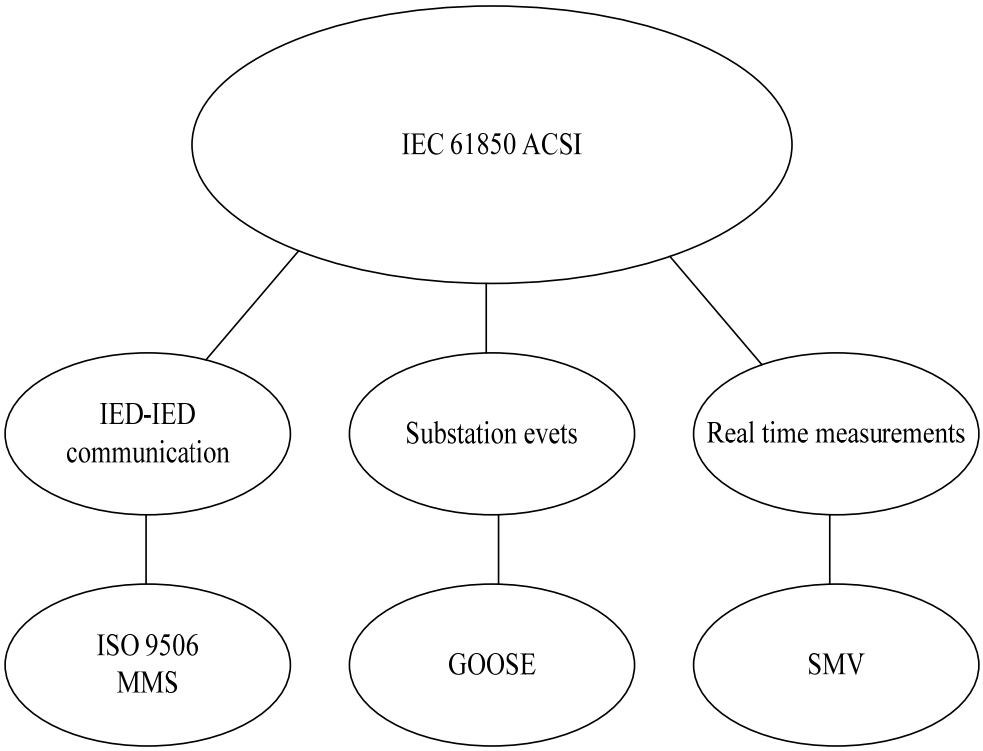


Figure 12.6: IEC 6180 ACSI protocol mapping

In addition to mapping data model to different protocols, IEC60850-6-1 defines the Substation Configuration Language (SCL). The SCL is based on the Extensible Markup Language (XML). The SCL uses three main files, the System Specification Description file (SSD), IED Capability description file (ICD) and Configured IED Description file (CID). Other types of files are used by SCL, such as Substation Configuration

Description file (SCD). The SCD file consists of s SSD file and ICD files [153]. Figure 12.7 shows the design and configuration process using SCL.

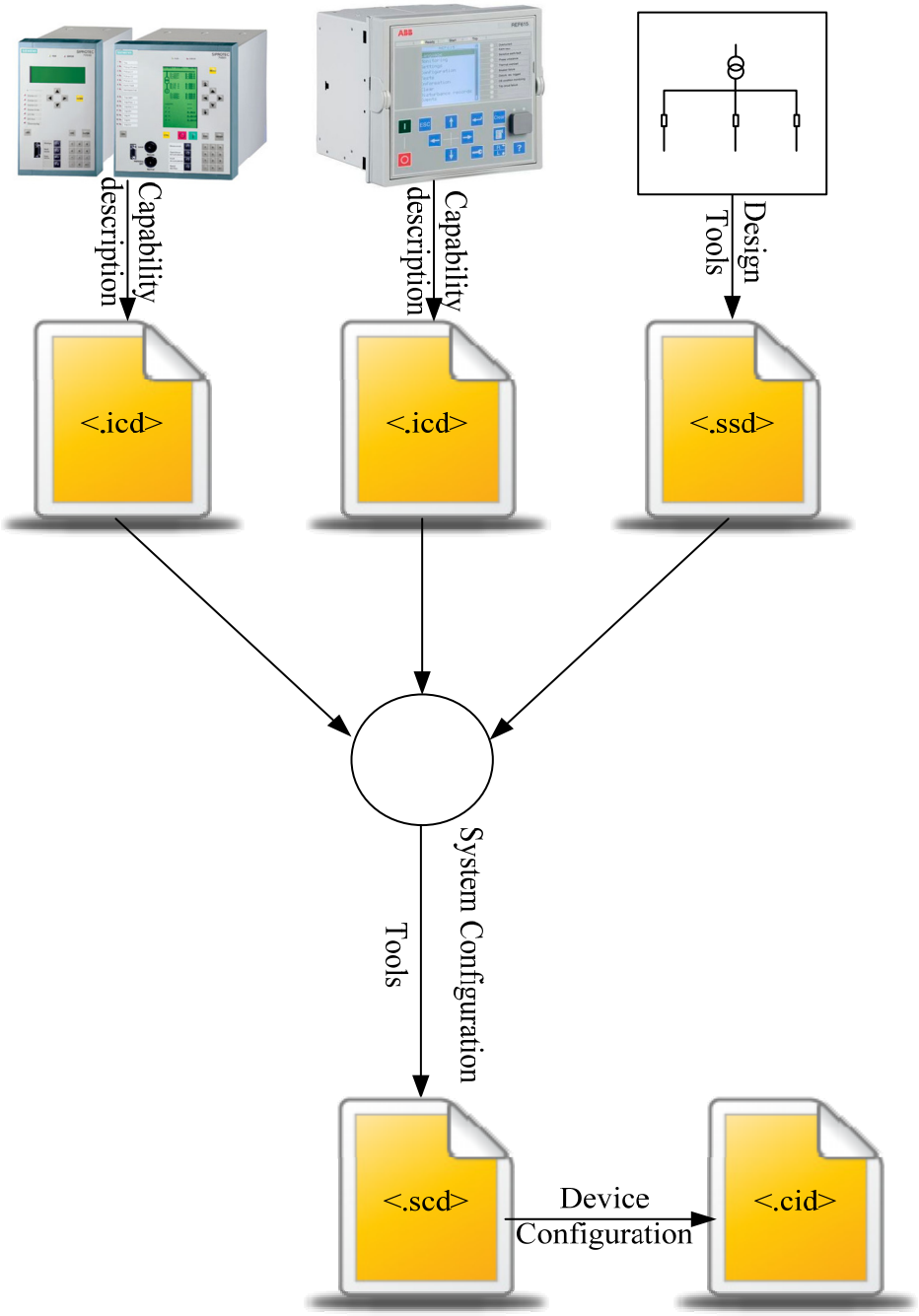


Figure 12.7: substation automation system designs and configurations process based on SCL

First, The SSD file is generated by the design tool. The SSD file defines the single line diagram for the substation, logical nodes and complete system specification. Based on the data from SSD and ICD, the system configuration tool defines the IEDs' logical nodes and the data flow and generates the SCD file. The SCD file contains a full description of the entire system. The SCD file is used by the device configuration tool to generate and load CID configuration files to individual IEDs.

12.3 IEC 61850 security

Evolving substation automation systems from legacy analog and serial interfaces to Ethernet-based network increases the risk of a cyber-attack. The attack surface ranges from inside person that infect the network with malware to supply chain, where the devices can be infected with suspicious software during manufacturing and installation [154]. The IEC 61850 doesn't specify any security measures to secure the IEDs and substation communication network. The security measures for the MMS, GOOSE and SMV messages are specified in IEC 62351 standard. The cyber threats, IEC security measures, and shortcoming are discussed in next sections.

12.4 MMS vulnerabilities

MMS messages are vulnerable to different types of known IP protocol attacks, such as address resolution protocol (ARP) cache poisoning attack, denial of service, a man in the middle attack and network flooding attack [155]. In the ARP poisoning cache attack depicted in Figure 12.8, the attacker uses spoofed ARP messages to deceive the victim and accept an invalid MAC (media access controller) address mapping and store it in

ARP cache. The invalid MAC mapping replaces the legitimate MAC with attacker MAC address.

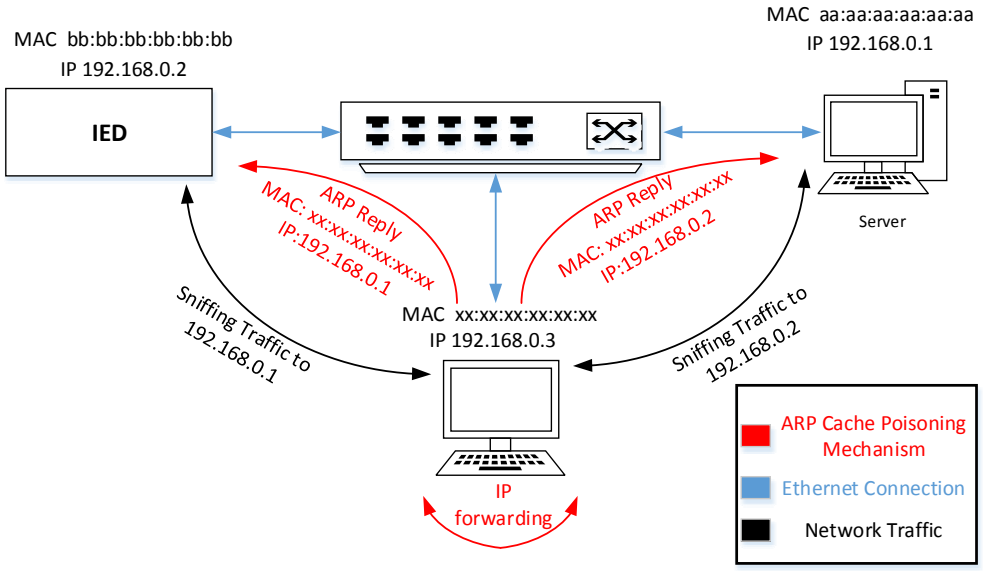


Figure 12.8: ARP Cache Poisoning Mechanism

Once the attacker replaces the legitimate MAC with his address, the network switch will redirect all IP packets to the attacker machine. The attacker can perform a man in the middle attack by modifying received packets and forward them to the victim machine. If the attacker didn't forward the received packet to the victim machine, it will cause a denial of service. Denial of service attack aims to prevent the device from providing the assigned service or exchanging the data with other devices. As mentioned earlier, such attack can be performed using ARP poisoning or by overloading the device with too many requests. Sending many requests to the network device could overload the processor and memory resource and could lead to stopping the service [155]. In the network flooding attack, the attacker sends a high rate of packets for network devices or

to a non-existing IP address, which consumes the network bandwidth and increases the communication delay.

12.5 GOOSE Message analysis and vulnerabilities.

GOOSE and SMV messages are sent directly to multicast MAC address on layer 2. Since the layer 2 message doesn't use The IP protocol for message routing, it's not prone to ARP poisoning attack. However, the attacker can still perform some types of attack based on the message anatomy and transmission method. Figure 12.9 shows the structure of the GOOSE message.

<table>
<tr><td colspan="2">Destination MAC Address</td><td colspan="2">Source MAC Address</td><td colspan="3">Priority Tagging/VLAN ID</td></tr>
<tr><td colspan="2">Ethertype (88B8)</td><td colspan="2">APPID</td><td colspan="3">Length</td></tr>
<tr><td colspan="2">Reserved 1</td><td colspan="2">Reserved 2</td><td>Tag</td><td>Length</td><td>goosePDU</td></tr>
<tr><td>Tag</td><td>Length</td><td colspan="2">gocbRef</td><td>Tag</td><td>Length</td><td>timeAllowedtoLive</td></tr>
<tr><td>Tag</td><td>Length</td><td colspan="2">datSet</td><td>Tag</td><td>Length</td><td>goID</td></tr>
<tr><td>Tag</td><td>Length</td><td colspan="2">t</td><td>Tag</td><td>Length</td><td>stNum</td></tr>
<tr><td>Tag</td><td>Length</td><td colspan="2">sqNum</td><td>Tag</td><td>Length</td><td>test</td></tr>
<tr><td>Tag</td><td>Length</td><td colspan="2">confRev</td><td>Tag</td><td>Length</td><td>ndsCom</td></tr>
<tr><td>Tag</td><td>Length</td><td colspan="2">numDatSetEntries</td><td>Tag</td><td>Length</td><td>allData</td></tr>
<tr><td>Tag</td><td>Length</td><td colspan="2">Data 1 (Boolean)</td><td>Tag</td><td>Length</td><td>Data 2 (Float)</td></tr>
<tr><td colspan="3">●●●●●● ●●●●●●</td><td>Tag</td><td>Length</td><td>Data N</td></tr>
</table>

Figure 12.9: Structure of a GOOSE Datagram

ALL GOOSE messages start with the destination's MAC address, followed by source MAC address, Priority Tagging/VLAN ID, Ethernet type, APP ID, Length and two reserved fields. These fields are described as the following:

- Destination MAC address: GOOSE messages use multicast MAC address as the destination address. The GOOSE multicast address must start with 01-0C-CD-01-xx-xx. The first three octets are (01-0C-CD) reserved for IEC 61850 protocol. The fourth octet is set to (01) for GOOSE messages.
- Source MAC address: this field contains the MAC address for the publisher IED.
- Priority Tagging/VLAN ID: GOOSE messages contain IEEE 802.1Q VLAN ID. The IEEE 802.1Q standard supports virtual LANs on an Ethernet network. The IEEE 802.1Q VLAN ID consists of Tag Protocol Identifier (TPID) and Tag control Identifier (TID). The TID is divided to Priority code point (PCP), 1-bit Drop eligible indicator (DEI). This indicator specifies if the message can be dropped in the case of congestion and 12-bit VLAN identifier field.
- Ether type: all GOOSE messages have a unique ether type field equal to 88B8.
- APPID: this field is used by the subscriber IEDs to identify the messages they are subscribing to.
- Length field: The Length field represents the length of the datagram minus eight bytes.
- Two reserved fields: these fields are reserved by the standard for future use.

A GOOSE message also has an IEEE 802.1Q VLAN ID, a unique Ethernet type, and an APPID field which subscribing IEDs use to identify the messages they are subscribing to. The Length field represents the length of the datagram minus eight bytes; the length field is followed by two reserved fields, which the standard leaves for future use.

The goose PDU is composed of twelve subfields, which are described as the following [156]:

- gocbRef: GOOSE control block reference
- timeAllowedtoLive: The time a receiver waits before receiving a re-transmitted message
- datSet: Name of the dataset.
- goID: ID of publishing IED.
- t: Timestamp indicating a new GOOSE event.
- stNum: Counter that increments with every GOOSE event.
- sqNum: Counter that increments with every repeated GOOSE message.
- test: Specifies if a message is intended for testing or not.
- confRev: Number of times the data set has changed.
- ndsCom: Needs commissioning field.
- numDataEntires: Number of data elements in allData.

- allData: Actual data being sent (bool, integer, float, etc.).

Since the publisher IED uses a multicast address to publish the GOOSE message, there is no way to ensure the message is received by all subscribers. To overcome this problem, the IEC 61850 implemented adaptive transmission time for GOOSE messages depicted in Figure 12.10. When an event occurs, the IED increments the stNum Counter and sends a GOOSE message as soon as possible. To increase the possibility of delivering the message to all subscribers, the Publisher retransmits the Message with the incremental time period. The publishers increment the sqNum with each transmitter. The timeAllowedtoLive field contains the time period before next retransmission.

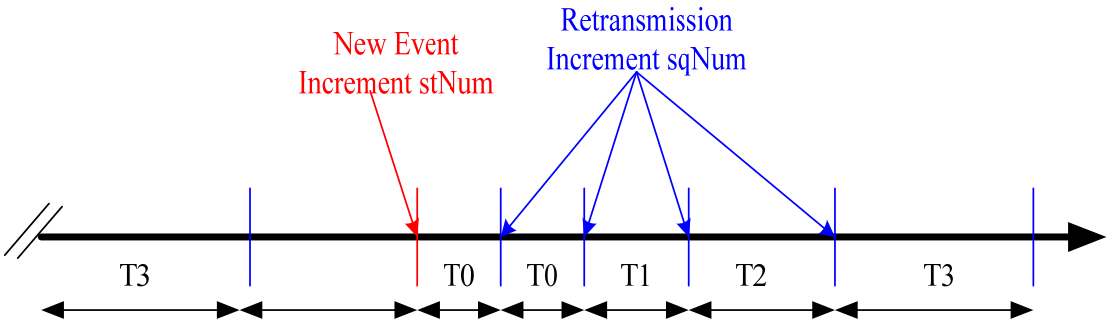


Figure 12.10: Adaptive GOOSE transmission time

GOOSE messages are prone to spoofing, replay, poisoning, and flooding attacks [157]. In the spoofing attack, the attacker uses a spoofed MAC address to multicast a fake GOOSE message with a manipulated data field. The attacker can get access to the GOOSE virtual LAN by VLAN hopping attack. After gaining access to the VLAN, the attacker monitors the network to capture a goose message and decode the message to

identify the data field and stNum. Then the attacker constructs and transmits the fake message with incremented stNum, as shown in Figure 12.11.

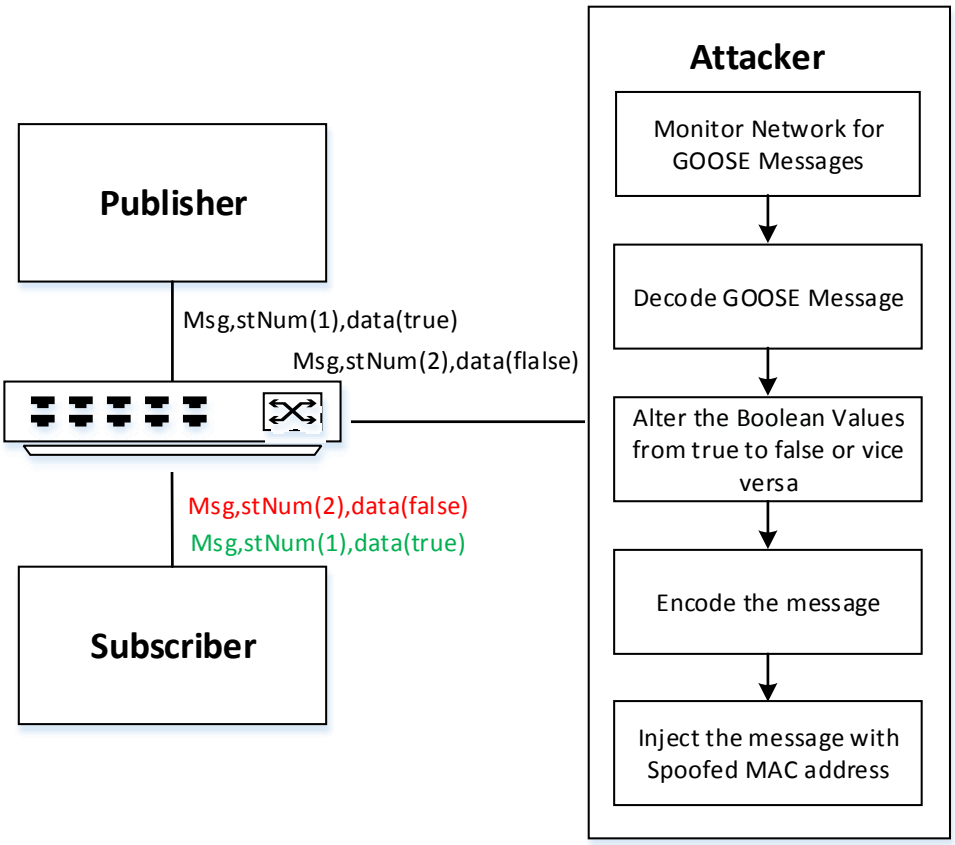


Figure 12.11: Spoofed GOOSE message attack

The spoofing attack can cause serious damage to the substation. For example, the attacker can change a Boolean field to trip or close a circuit breaker and energize the wrong circuit. A replay attack is similar to the spoofing attack except that, instead of constructing the fake message, the attacker records previous events and replays it later with a spoofed MAC address. To prevent a replay attack, the subscriber should discard any message with a stNum less than or equal to the previous message until a rollover

occurs, as specified by IEC 62351 standard. However implementing stNum checks lead to another type of serious attack, which is GOOSE poisoning attack.

In GOOSE poisoning attack, the attacker sends a message with a high stNum number. If the stNum check is implemented the subscriber will discard all legitimate messages with a lower stNum number [158]. GOOSE poisoning attack has the same impact as denial of service attack but is more dangerous. Regular denial of service attack depends on sending a huge number of messages to overload the receiver. GOOSE poisoning attack can cause the same impact with transmitting a single packet, which makes it harder to discover. Since the SMV messages use Layer two Multicasts as GOOSE messages, it is also prone spoofing, and reply attack.

12.6 IEC 62351 Security Standard

As mentioned earlier, the IEC 61850 doesn't specify any security roles for the substation automation network. The IEC 62351 is the standard that provides security to a number of TC57 protocols, including IEC 61850. It was developed by TC57, the same technical committee that developed IEC 61850, WG15 in 2007. Its objectives were to prevent eavesdropping and spoofing attacks, detect intrusions, and authenticate data transfers through digital signatures. The IEC 62351 standard is divided into 11 parts that cover security for different protocols. Parts 3, 4 and 6 are the parts related to the IEC 61850 security. IEC 62351-3 defines the security for profiles including TCP/IP. IEC 62351-4 defines the security rules for MMS, while IEC 62351-6 focuses on GOOSE message security. IEC 62351-3 requires TLS for all TCP/IP-based communications. This is done in order to protect against eavesdropping, spoofing, replay attacks and some

modification attacks [159], but it fails against denial of service attacks [160]. This section also requires node and message authentication through the use of digital signatures [161]. IEC 62351-4 requires TLS and authentication specifically for MMS. MMS traffic is done on the application and transport level. Security on the application level is done using peer authentication which is accomplished by carrying authentication information in the ACSE AARQ. It also includes AARE PDUs Authentication is made up of an X.509 encoded certificate, time stamp, and digitally signed time value. Security on the transport level refers to TLS and specifies the minimal mandatory and recommended cipher suites to be used, TLS_DH_DSS_WITH_AES_256_SHA and LS_DH_RSA_WITH_AES_128_SHA[162]. IEC 62351-4 allows usage of secure and non-secure profiles. This feature allows operation in systems that are not fully upgraded to new security measures. To cover the communication security of IEC 61850's peer-to-peer profiles (GOOSE), IEC 62351-6 was created. The digital signatures and encryption methods provided for other types of messaging require a lot of time to be generated and verified. Therefore, section 4 states that "for applications using GOOSE and IEC 61850-9-2 and requiring 4 ms response times, multicast configurations and low CPU overhead, encryption is not recommended" [154]. The only required security measure for GOOSE messages is message authentication. The message authentication is defined by extending the GOOSE Protocol Data Unit (PDUs) with an authentication value. This authentication value is calculated by signing an SHA256 hash using RSA. Certificate exchange is not done with these messages. All X.509 encoded certificates must be pre-installed on the receiving nodes [162]. However, a study performed in [163] showcased that applying asymmetrical encryption to multicast GOOSE and SMV messages while meeting the 4ms

time constraint imposed by IEC 61850-9-2 is practically unfeasible with current IED processor technologies, even if implemented on high-end, expensive hardware. This left IEC 62351-6 with little industry acceptance. This leaves GOOSE messages with no encryption and no authentication. Given all the efforts by IEC 62351, the lack of data encryption paves the way for attackers.

12.7 Implementation vulnerability

System vulnerabilities can result from standard shortcoming, misconfiguration and different vendors' implementation for the standard. Vendors' implementation could have software bugs or drift from the original standard. Two different implementations of the IEC 61850 were tested and analyzed to identify possible vulnerability and drift from the original standard. The first platform is the LIBIEC61850 open source library. LIBIEC61850 is a C library that provides MMS, GOOSE and SMV implementation, which utilized in a different commercial product. The platform is a commercial IEC 61850 protection relay available at the Smart Grid test bed at Florida International University. Three tests were performed to verify the proper implementation of GOOSE messages' stNum, Timestamp, and source MAC address fields processing algorithm [156].

In the stNum processing test, GOOSE messages are transmitted to both devices with different stNum values. First, a message with stNum equal to 2 is transmitted, then followed by a message with lower stNum, as shown in Figure 12.12. Each message has a Boolean field which trips a digital output. Changing the digital output state indicates that the IEDs process the message, while fixed output indicate the message is discarded. In

this test, the LIBIEC61850 discarded the message with lower stNum as specified by the standard while the commercial relay processes the message and triggers the digital output.

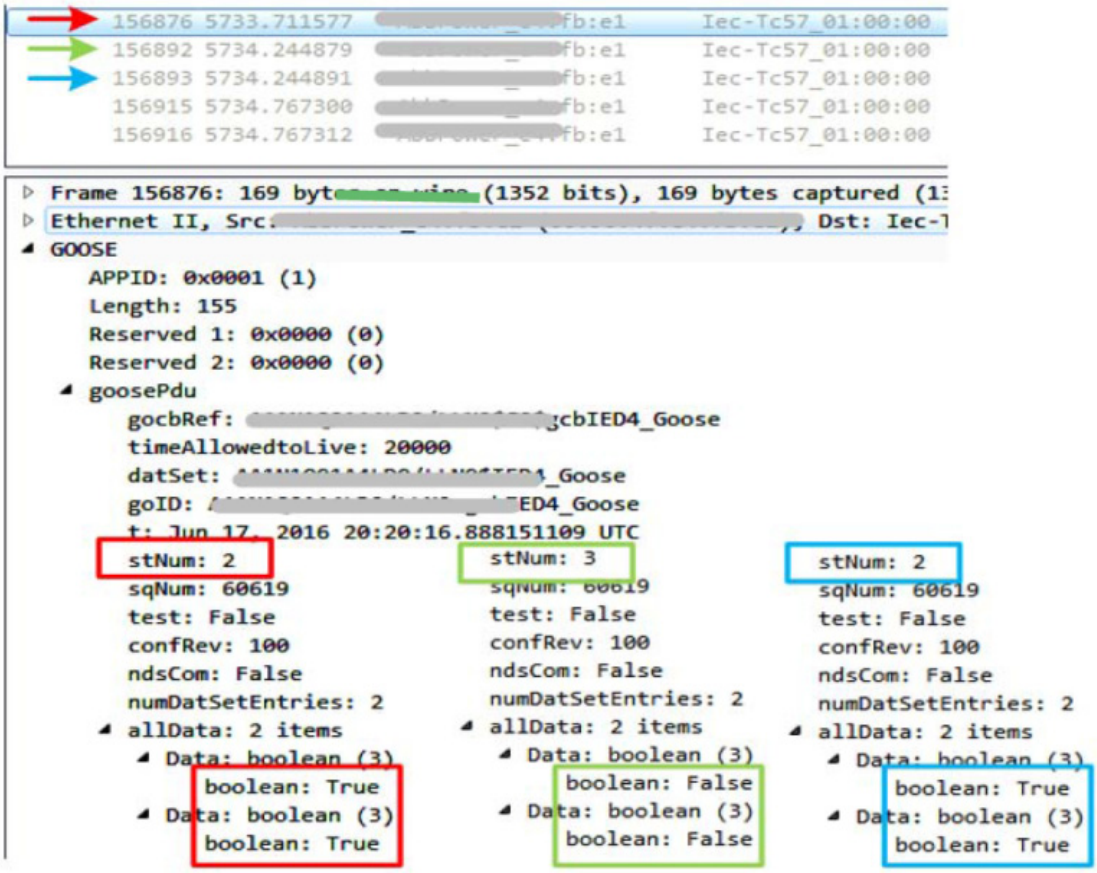


Figure 12.12: Goose messages with two different stNum

In the time stamp processing test, a GOOSE message with an old timestamp (three days) is transmitted to both platforms, as shown in Figure 12.13. In this test, both platforms process the message and change the digital output state. It is noteworthy to point out that, IEC 61850 recommends checking for a message's time stamp only if it recognizes a stNum different than that of the previous message. The experiments revealed that when sending new messages with three-day-old time stamps exceeding the

2-min skew, they were processed as long as they had status numbers equal to or higher than the previous message. In the source MAC address processing test, a message with invalid Source MAC address is sent to both platforms under test. Both platforms processed the message with the invalid source address.

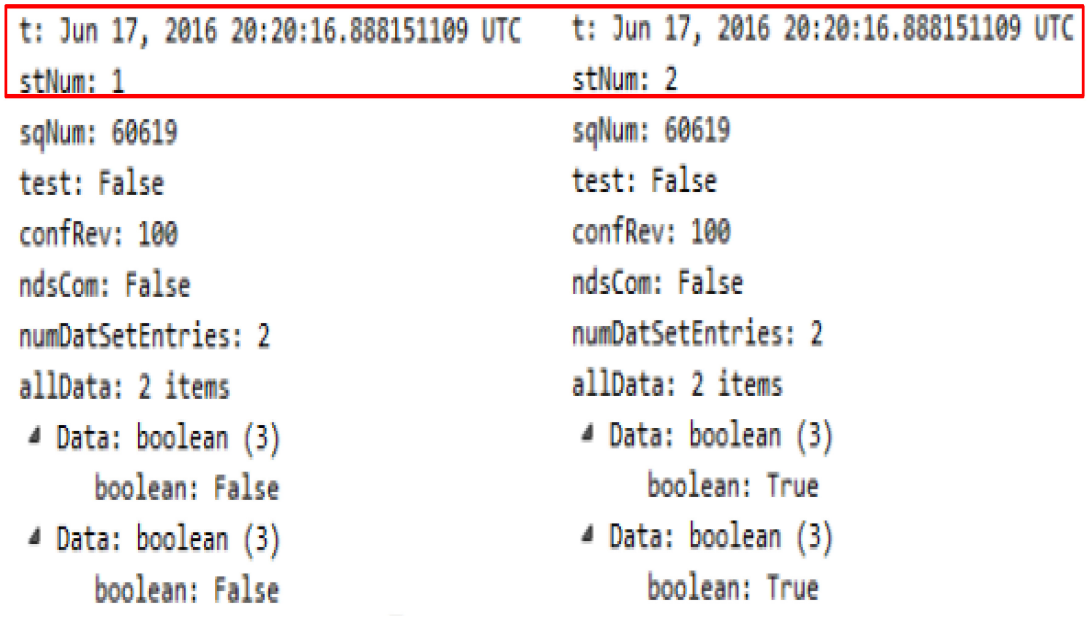


Figure 12.13: Outdated GOOSE message content

This test actually exploits a vulnerability in the GOOSE messaging protocol itself rather than its implementation in commercial devices. In the GOOSE protocol, subscribing IEDs use the APPID field to subscribe to the desired GOOSE messages. Since the subscribing IEDs, in this case, do not check for the source MAC address, they will process any message with their defined APPID, regardless of its origin.

Table 12-1 summarizes the results of the performed tests on both the commercial IEDs and libiec61850.

Table 12-1: Compliance Test Results.

Test	Commercial IED	LIBIEC61850	Standard specification
Lower stNum processing	Y	N	Discard
Outdated time stamp processing	Y	Y	Discard
Invalid MAC address	Y	Y	Not specified

12.8 Summary

In this chapter, a security analysis and investigation of the IEC 61850 substation automation protocol and IEC 62351 security protocol is presented. While The IEC 61850 migrate the substation automation system toward high-speed Ethernet network and provide the necessary data modeling and interoperability standard, it doesn't specify any security measures to protect the IEC 61850 protocols. The IEC 62351 specifies the security measures for the MMS, GOOSE and SMV protocols, but the analysis shows that IEC 62351 is not the ultimate solution for cyber invasions on substations. IEC 62351 fails to protect GOOSE and SMV messages from the cyber-attacks. IEC 62351-6 proposes the use of digital signatures through the RSA algorithm to ensure the integrity of multicast GOOSE and SMV messages, which is not feasible due to time constraint and hardware limitation. The experimental testing shows that vendors' implementation could introduce some vulnerability, such as improper processing of stNum and time stamp fields. This improper implementation allows replay attacks, while the proper implementation according to the standard enables the GOOSE poisoning attack. A security algorithm to

secure GOOSE and SMV layer 2 messages, and discard fake messages, while meeting the 4ms delay time constraint, is required.

Chapter 13 Sequence Hopping Security Mechanism For Energy Systems

13.1 Introduction

Modern power system automation and the smart grid rely on communication for various reasons, including critical infrastructure protection and power routing. Communication between substation IED devices is integral for substations to keep up with their real-time operations. IEDs perform several protective and control functions in a substation automation system, such as data and file transfer. Unfortunately, whenever data are transferred, there is an opportunity for the data to be intercepted or corrupted. In addition, data can be sent from or intercepted by malicious and unauthorized sources, potentially causing catastrophic consequences. The industry has established data security protocols in an attempt to avoid the intrusion of malicious and unauthorized sources. However, these protocols often require intensive processing power for which existing, and even some modern IEDs, are not equipped to handle, as discussed in the previous chapter. Adding to the problem, some of the critical data sent between IEDs needs to be transmitted quickly, limiting the amount of encryption/decryption time and further increasing the processing requirements of IEDs. This combination of IEDs lack of processing power and the need for critical information to be relayed quickly has resulted in critical data being transmitted unprotected, leaving an opening for unauthorized and potentially malicious users to cause harm to the system. In this chapter, a security mechanism based on the sequence hopping number will be developed to secure the IEC 61850 GOOSE messages. The developed mechanism uses minimal processing resources and secures the GOOSE messages without violating the 4 ms time delay restriction.

13.2 GOOSE messages vulnerabilities and attack surface

GOOSE messaging protocol was developed for applications that require a fast and reliable information exchange with strict time constraints within the boundaries of a substation. However, recently, IEC 61850 has been extended to cover applications that require inter-substation communication such as tele-protection which utilizes GOOSE messages over WAN. Therefore, the criticality of the GOOSE messaging protocol is inherited from the applications it is implemented in. GOOSE messages should be handled with care because any misconfiguration might lead to devastating consequences, ranging from system instabilities to complete blackouts.

The IEC 62351-6 devises an algorithm for proper processing of GOOSE messages in order to mitigate some cyber-attacks such as replay attacks. From the publishing IED side, each GOOSE message has a status and sequence number field (stNum and sqNum, respectively). When a substation event occurs, for example, an overcurrent is sensed, the publishing IED instantly transmits a message with an incremented stNum field. The message is then repeated with variable increasing time delay until the maximum defined period is reached. The sqNum counter increments with every repeated message until the maximum number count (2^32-1) is reached; the point at which the sqNum counter rolls over. IEC 62351-6 states that a subscriber IED, which detects a new message with a new stNum, must discard any message having a stNum less than that or equal to the previous message and which time allowed to live hasn't timed out yet, unless a rollover of the stNum counter occurs. If none of the conditions above are true, the subscribing IEDs process the messages.

The processing of state numbers set by IEC 62351 to counter replay attacks makes the system prone to Denial of Service and GOOSE poisoning attacks. Since GOOSE messages travel the network unencrypted, an attacker can monitor the network and deduce the current state number. The attacker can then send a message with a very high-status number, as discussed in the previous chapter. All the subscribing IEDs will then discard messages from authenticated IED because they will have a lesser status number than that published by the attacker. Also, the standard's solution for data integrity using RSA digital signatures will not meet the 4ms time constraint imposed on GOOSE messages given the low processing power of current IED processors. Recent studies also show that digital signatures fail to meet the 4ms time constraint on more advanced processors [162].

The IEC 61850 uses a multicast MAC address to transmit the GOOSE message over Layer 2; therefore the attacker can't use ARP poisoning attack to redirect the message to an intermediary device or block the message delivery. The only way to manipulate a message is by resending a modified copy of the message.

The attack surface for the GOOSE messages can be summarized in the three different methods as below:

- Sending a fake message with incremented stNum.
- Retransmitting old message after manipulating data field (spoofing attack).
- Sending a fake message with very high stNum (GOOSE poisoning attack).
- The security mechanism should provide a way to prevents these types of attack and validate the message content without violating the 4ms restriction.

13.3 Sequence hopping security mechanism

A keen analysis of the GOOSE messages' vulnerabilities reveals that the vulnerabilities result from two main sources. The first factor is sequential nature of the stNum field; incremented stNUM field allows the attacker to easily construct and transmit a fake or manipulated GOOSE message with the correct stNum. The subscriber will process the message as long as it contains a new stNum field. The second factor is the lack of the source verification mechanism. IEC 61850 implements a publisher/subscriber communication scheme to deliver the GOOSE message, which is called connectionless communication. In this communication scheme, the subscriber subscribes to the message by the APPID only. The IEC 61850 doesn't provide a method to verify the data source. The attacker can send a GOOSE message with spoofed or completely different MAC address and the subscriber will receive and process the message as long as it contains the correct APPID and stNum fields. The proposed sequence hopping mechanism solves the vulnerabilities issues resulting from these factors. The sequence hopping security mechanism is inspired by the frequency hopping technique which was developed for securing military communications. In the frequency hopping communication, the transmitter transmits the data by rapidly changing the channel frequency among different channels' frequency with a pseudo-random pattern know to both the transmitter and receiver. The frequency hopping systems implement synchronization algorithms to synchronize the transmitters and the receivers' pseudo-random pattern. In the sequence hopping security mechanism, we are proposing the addition of a new field to the GOOSE message called the HseqNum or the "hopping sequence number" and incremental counter. Each of the publishing and receiving IEDs

will have synchronized pseudo-random generators (PRNG) fed with the same seed by a secure mechanism explained in the next section. Therefore, synchronized generation of the same random number will occur inside the publisher and the subscriber. The subscriber will only accept messages possessing a matching HseqNum as that generated by its PRNG. Any message with a repeated or unmatched HseqNum will be discarded. In order to send a fake or manipulate a message, the attacker needs to know the next correct HseqNum. Since the HseqNum is random and unique for each message, the attacker will not be able to predict the next valid HseqNum. The proposed security mechanism is composed of A Message Sequence Synchronization and Monitoring Server (MSSMS) and synchronization clients, shown in Figure 13.1.

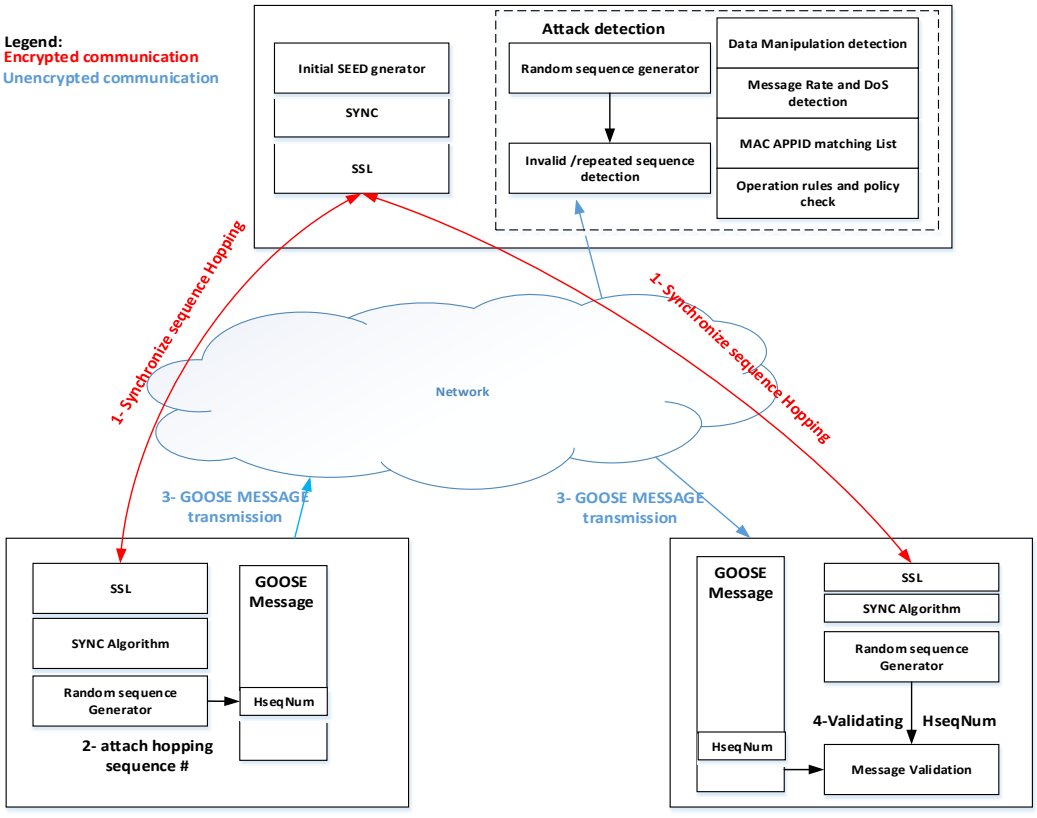


Figure 13.1: Sequence hopping security mechanism block diagram

The description and operation of the MSSMS and synchronization clients are discussed in details in the next sections.

13.3.1 Message sequence synchronization and monitoring server (MSSMS)

The MSSMS is the core component in the sequence hopping security mechanism. The MSSMS will be responsible for synchronizing all PRNG in publisher and subscriber IEDs. The MSSMS will use an encrypted connection for synchronization and exchange of the initial seeds with all nodes through SSL connection. Although the messages are unencrypted, the mathematical complexity of the PRNG is extremely hard to reverse without a long sequence of numbers. The MSSMS server will generate new seeds before enough numbers were generated for discovering the currently utilized seed by correlation. In addition to the synchronization task, The MSSMS will perform a monitoring task to detect possible attacks and intrusion as described below.

Data manipulation detection: The MSSMS server monitors published GOOSE messages stNum, sqNum and data fields. If the SMMS detects messages with new sqNum but has a modified data field, it will generate an alarm signal.

Fake message attack detection: To detect any attempt to send fake messages from a machine inside the network, the MSSMS will have a list of MAC addresses and their association APPID. The MSSMS will keep track of the association of APPIDs with the source MAC address of the message in order to prevent sending fake GOOSE messages from unauthenticated devices.

Detect attack on the sequence hopping mechanism: For early detection of any attempt to attack the sequence hopping mechanism, the MSSMS server will monitor the HseqNum field in published messages. If a repeated or out of order HseqNum is detected, the MSSMS server will generate an alarm.

Physical and operation rules check. MSSMS will have a defined set of rules that represents physical and operation restrictions. The server will check the GOOSE message content and generate an alarm signal if the GOOSE content violates one or more of the predefined rules. The message content will be validated by pre-defined policies related to the substation operation scenarios. For example, if a power circuit is disconnected for maintenance, the MSSMS server will consider any message with content intended to energize this circuit as an invalid message and will eventually send an alarm signal.

The MSSMS server utilizes a multithreading to handle multiple simultaneous connections. The server is developed using C programming language and run under Ubuntu Linux.

13.3.2 PRNG synchronization process

To secure the GOOSE messages, the following steps, shown in Figure 13.1 and detailed below, will be performed:

1- The MSSMS server will generate a sequence of random seeds.

2- Upon joining the network, a publisher IED will initiate an encrypted communication channel with the MSSMS server. This encrypted channel will be used to exchange the random seed with the publisher.

3- The publisher IED will use the randomly generated seed to generate a new sequence hopping number and attach it to each transmitted message. The flowchart of the publisher synchronization process is shown in Figure 13.2.

4- The MSSMS will synchronize all the subscriber IED devices with the same random pattern as well.

5- The subscriber will expect that the unique hopping sequence number for each received message will match with its internal synchronized sequence.

6- Any message with invalid or repeated sequence number will be discarded. The flowchart for the steps 4, 5 and 6 is shown in Figure 13.3.

7- The MSSMS server will synchronize the devices periodically with a new pattern to avoid discovering the random pattern.

8- After the synchronization process, the MSSMS server will monitor the messages published by IEDs for possible attacks.

9- The MSSMS will monitor the messages' publishing rate, check their sequence hopping field for repeated or invalid patterns and check the message content against pre-defined operation rules.

13.3.3 SSL encryption

The communication between the MSSMS server, publisher IEDs, and subscriber IEDs are secured using secure socket layer communication. The OpenSSL library is used to implement the SSL communication. To generate a digital certificate for the publisher

and subscriber, a certificate authority (CA) is created for the energy systems research lab (ESRL CA). The ESRL CA issues and signs the certificates for the publishers and subscribers IEDs. The ESRL CA root certificate is used to verify the IEDs' certificates. Figure 13.4 and Figure 13.5 show the CA certificate and signed IEDs certificate, respectively.

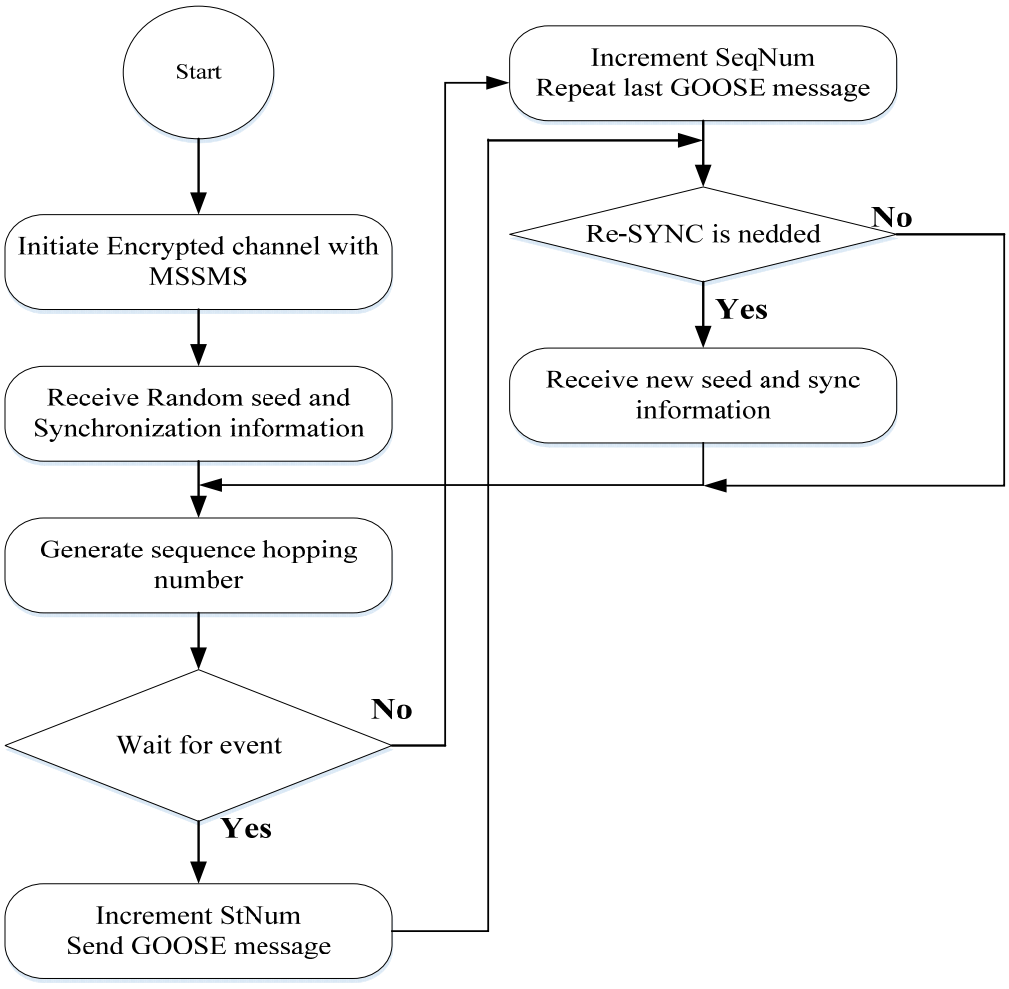


Figure 13.2: Publisher synchronization flowchart

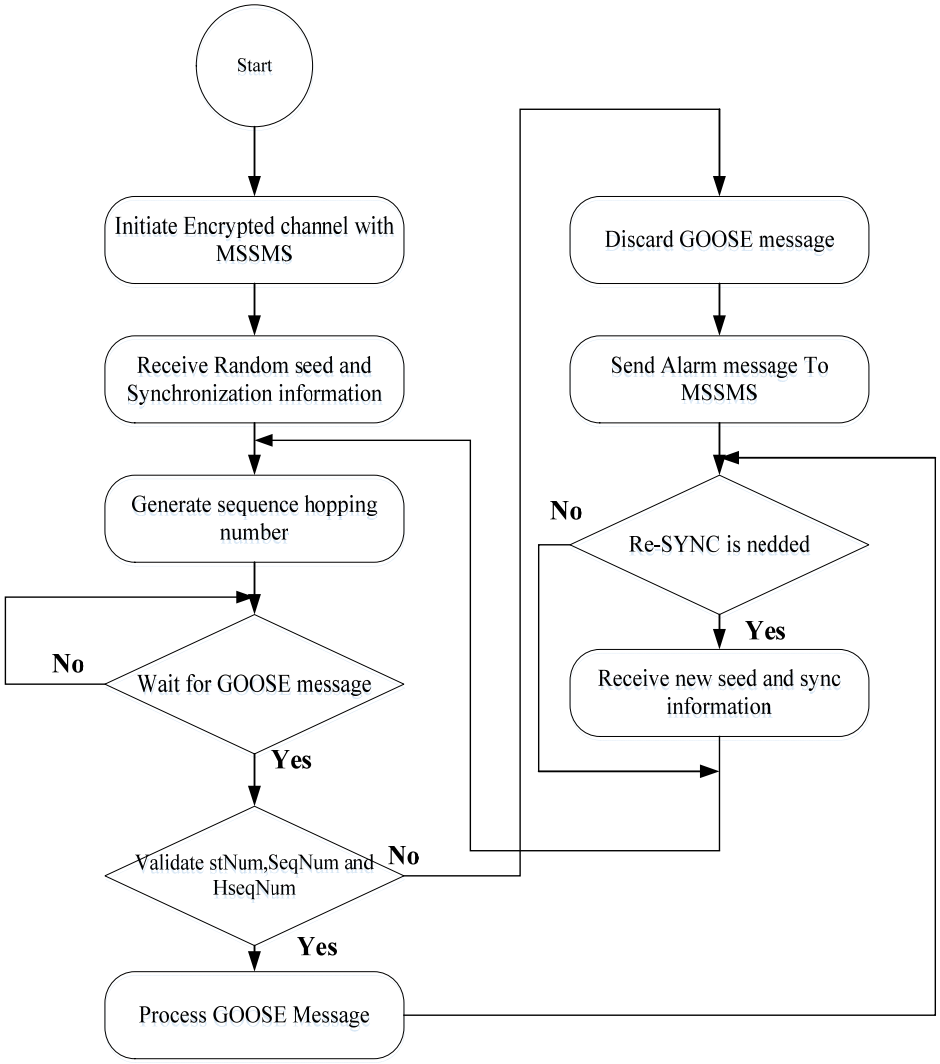


Figure 13.3: Subscriber synchronization flowchart

In standard internet application, the client verifies the server identity by receiving and validating its certificate using the CA certificate. This single-side validation is not enough in this application. For complete security, the client needs to validate the server identity before synchronizing the random sequence and the server must validate the client identity before revealing the seed

ESRL Root Certificate Authority

Identity: ESRL Root Certificate Authority
Verified by: ESRL Root Certificate Authority
Expires: 07/25/2021

Details

Subject Name

CN (Common Name):	ESRL Root Certificate Authority
ST (State):	FL
C (Country):	US
EMAIL (Email Address):	tyous001@fiu.edu
O (Organization):	FIU
OU (Organizational Unit):	Smart Grid Testbed

Issuer Name

CN (Common Name):	ESRL Root Certificate Authority
ST (State):	FL
C (Country):	US
EMAIL (Email Address):	tyous001@fiu.edu
O (Organization):	FIU
OU (Organizational Unit):	Smart Grid Testbed

Issued Certificate

Version:	3
Serial Number:	00 F3 17 9D BC 56 55 19 ED
Not Valid Before:	2016-07-26
Not Valid After:	2021-07-25

Certificate Fingerprints

SHA1:	81 FF 84 8C 13 4A D5 32 83 B5 E9 87 40 44 11 CF AC 25 FF 2C
MD5:	F7 D6 AF FC 8F 01 C3 09 D8 D5 92 5E A4 48 55 C5

Figure 13.4: Root certificate

MSSMS_CL

Identity: MSSMS_CL
Verified by: ESRL Root Certificate Authority
Expires: 07/25/2021

Details

Subject Name

CN (Common Name):	MSSMS_CL
ST (State):	FIU
C (Country):	US
EMAIL (Email Address):	tyous001@fiu.edu
O (Organization):	FIU
OU (Organizational Unit):	Smart Grid Testbed

Issuer Name

CN (Common Name):	ESRL Root Certificate Authority
ST (State):	FL
C (Country):	US
EMAIL (Email Address):	tyous001@fiu.edu
O (Organization):	FIU
OU (Organizational Unit):	Smart Grid Testbed

Issued Certificate

Version:	3
Serial Number:	02
Not Valid Before:	2016-07-26
Not Valid After:	2021-07-25

Certificate Fingerprints

SHA1:	C6 95 AC A7 FA C9 2E 6D 5A 19 F6 C3 1F 78 05 A1 E1 2D 23 52
MD5:	B8 8F F4 70 78 5A 47 C6 01 A3 2B 4D 76 34 47 9D

MSSMS

Identity: MSSMS
Verified by: ESRL Root Certificate Authority
Expires: 07/25/2021

Details

Subject Name

CN (Common Name):	MSSMS
ST (State):	FIU
C (Country):	US
EMAIL (Email Address):	tyous001@fiu.edu
O (Organization):	FIU
OU (Organizational Unit):	Smart Grid Testbed

Issuer Name

CN (Common Name):	ESRL Root Certificate Authority
ST (State):	FL
C (Country):	US
EMAIL (Email Address):	tyous001@fiu.edu
O (Organization):	FIU
OU (Organizational Unit):	Smart Grid Testbed

Issued Certificate

Version:	3
Serial Number:	01
Not Valid Before:	2016-07-26
Not Valid After:	2021-07-25

Certificate Fingerprints

SHA1:	CD 20 E4 D3 27 92 E8 30 0F 31 F3 65 D6 E2 B1 D9 80 B3 F8 64
MD5:	84 03 E7 8B F7 98 C2 D0 78 64 3F D3 2A EC 8D B6

Figure 13.5: Client and server certificates

.

13.4 Experimental validation

The proposed sequence hopping security mechanism is implemented and verified experimentally. Two different types of implementation were tested. The first implementation assumes that the security mechanism will be embedded in the device's firmware or applied as a software upgrade for the IEDs. The second type of implementation adds the security feature to legacy devices as a bump in the wire solution.

In the embedded solution, two IEDs were developed to implement IEC 61850 GOOSE communication with an added security feature. The developed IEDs firmware is based on the open source libiec61850 and OpenSSL libraries. The IEDs' firmware run at ARM based single-board computer with 700 MHz clock. The benchmarking of the algorithm shows that the generation of the random sequence adds less than 0.015 ms delay. The total end-to-end delay including construction, transmission, receiving, decoding and validating the GOOSE message is 250 μs. To measure the end-to-end delay, a function generator is connected to the publisher digital input, as shown in Figure 13.6. The publisher IED is programmed to send a GOOSE message with the Boolean field when it detects a transition in the digital input. The subscriber IED receives the GOOSE message and changes the digital output status according to the value of the Boolean field after validating the message. The function generator and the subscriber output are captured using a digital oscilloscope to calculate the end-to-end delay time.

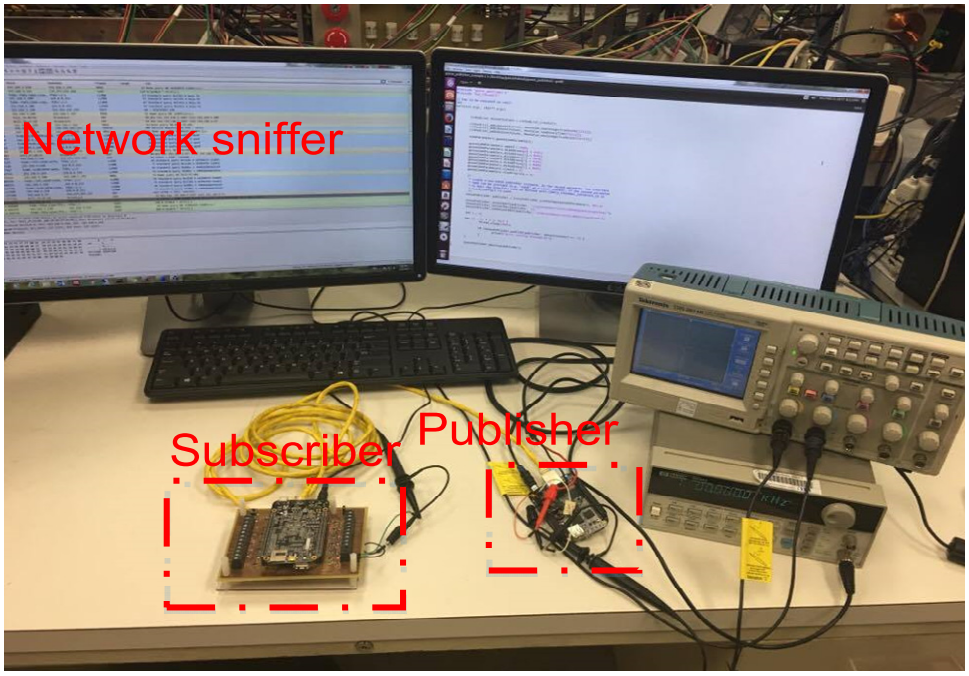


Figure 13.6: embedded sequence hopping security solution test setup.

Figure 13.7: End-to-end delay time for the embedded sequence hopping implementation.

In the bump in the wire solution, the sequence hopping security mechanism is implemented on two single-board computer, injection and verification boards, as shown in Figure 13.8. Each board has two Ethernet network interfaces. The first board (injection board) is connected directly to the publisher IED. The injection board synchronizes the random number generator with the MSSMS server, receives the original GOOSE message from the subscriber, inserts the HseqNum field and retransmits the message to the network.

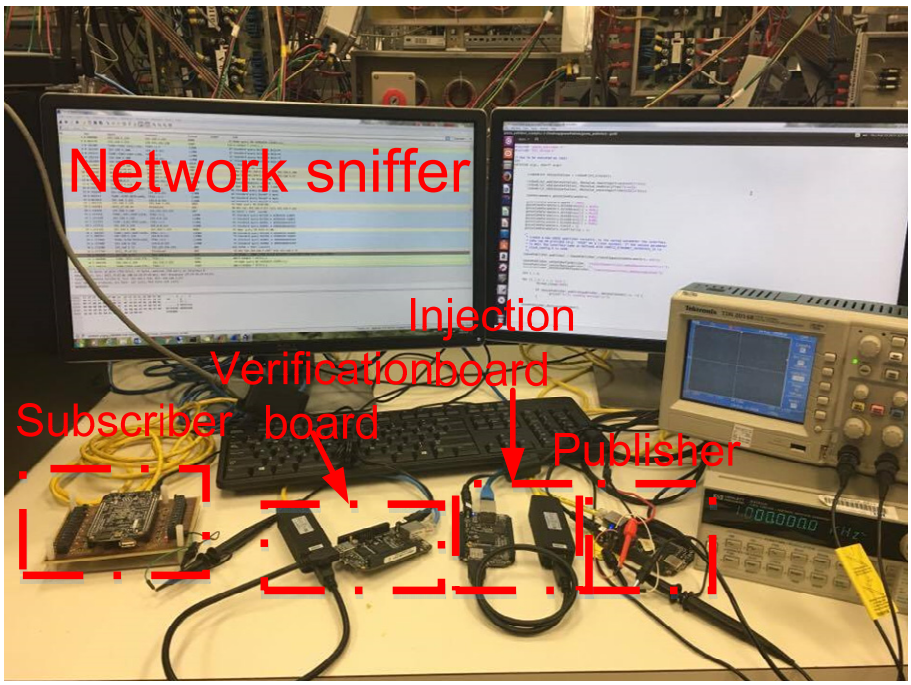


Figure 13.8: Bump in the wire sequence hopping security mechanism implementation setup.

Figure 13.9 shows the client and server outputs during the identity verification. Both MSSMS server and clients exchange the certificates, validate and print out the verified identity. The detailed SSL handshaking and communication is captured using Wireshark sniffing software and shown in Figure 13.10. The MSSMS server has the 192.168.5.53 IP

while the injection board has the 192.168.5.47 IP. As depicted from the figure, the MSSMS server and client use SSL V3.0 with AES 256 encryption. Both server and clients exchange certificates. After the handshaking, they established an encrypted communication channel.

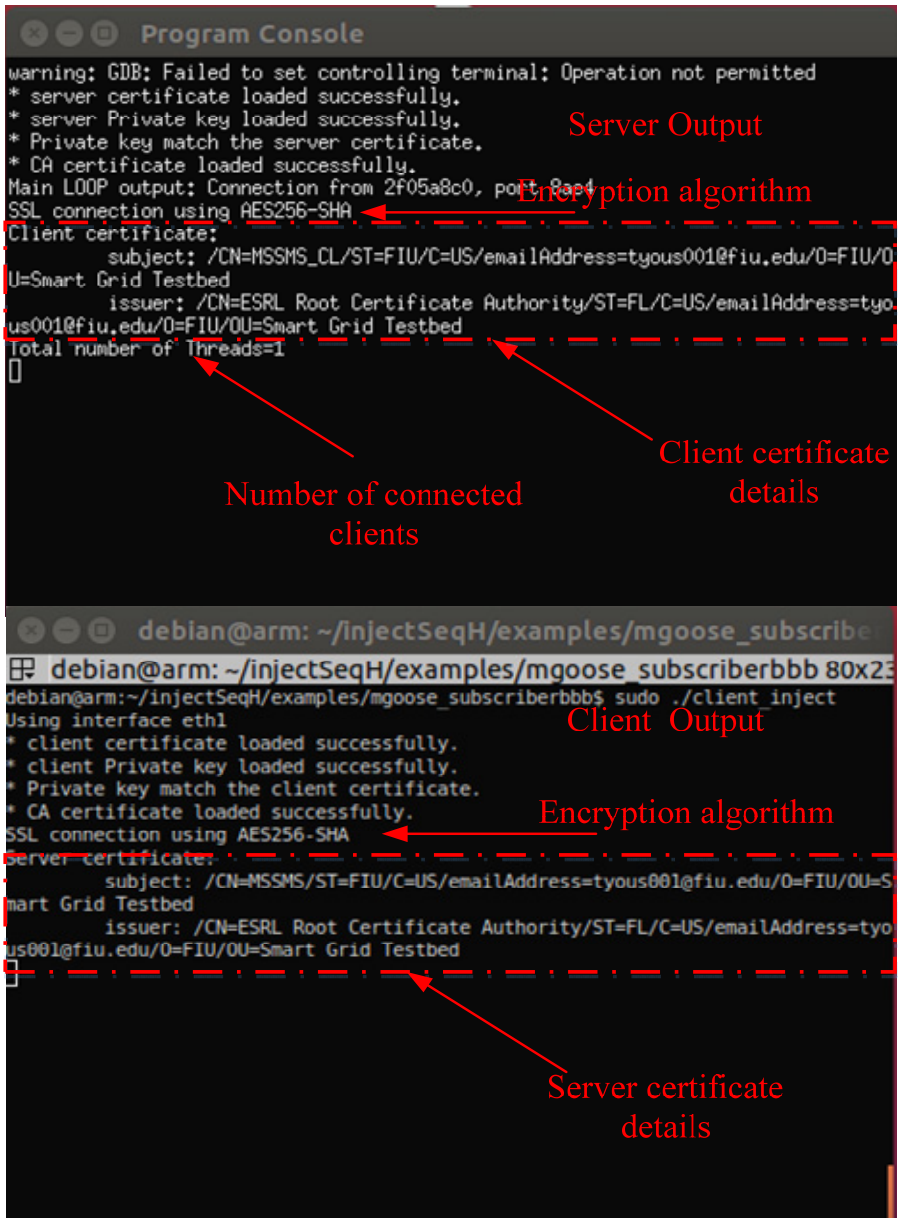


Figure 13.9: MSSMS server and client outputs during SSL initialization.

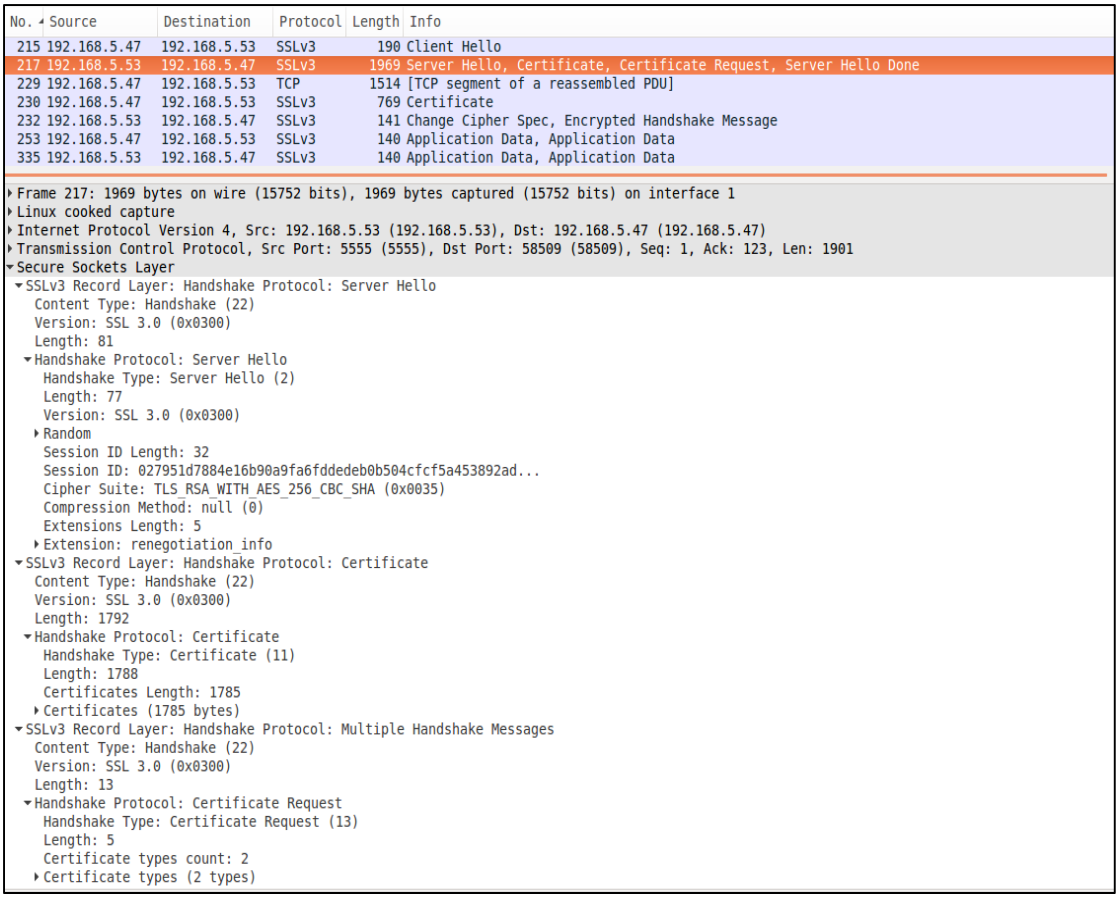


Figure 13.10: SSL handshaking

The original GOOSE message published by the legacy IED is shown in Figure 13.11. As depicted from the figure, the original GOOSE message has stNum equal to 50 and two true Boolean fields. The injection board inserts the HseqNum field with a value equal to 158971337, as shown in Figure 13.12. The injection board maintains the same time stamp, stNum, and sqNum as the original message. The total end-to-end delay is measured by calculating the time delay between the events (digital input status change) and the subscriber digital output status change. The input and output signals are captured using a digital oscilloscope, as shown in Figure 13.13. As depicted from the figure, the maximum end-to-end delay is 1 ms.

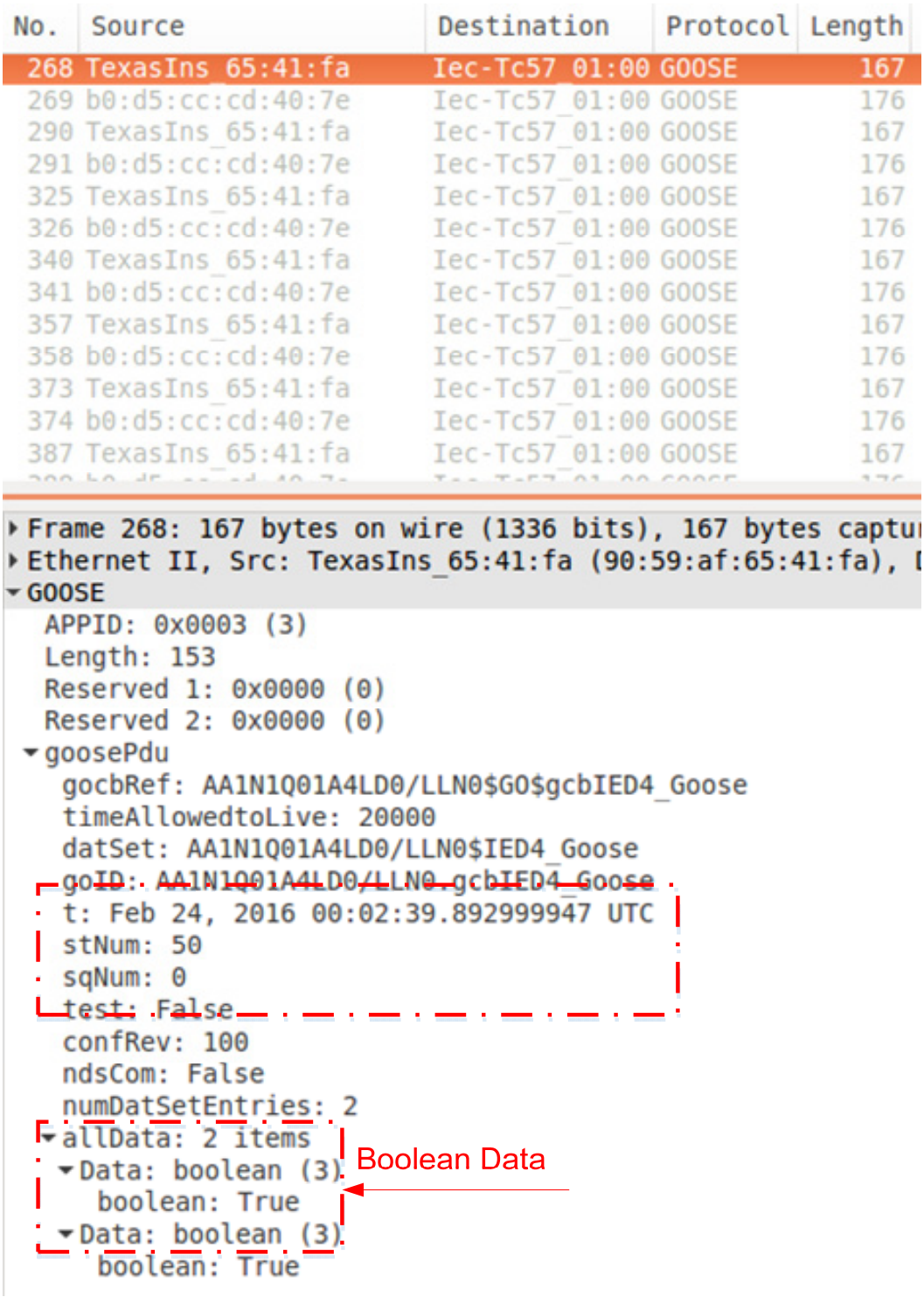


Figure 13.11: Original GOOSE message

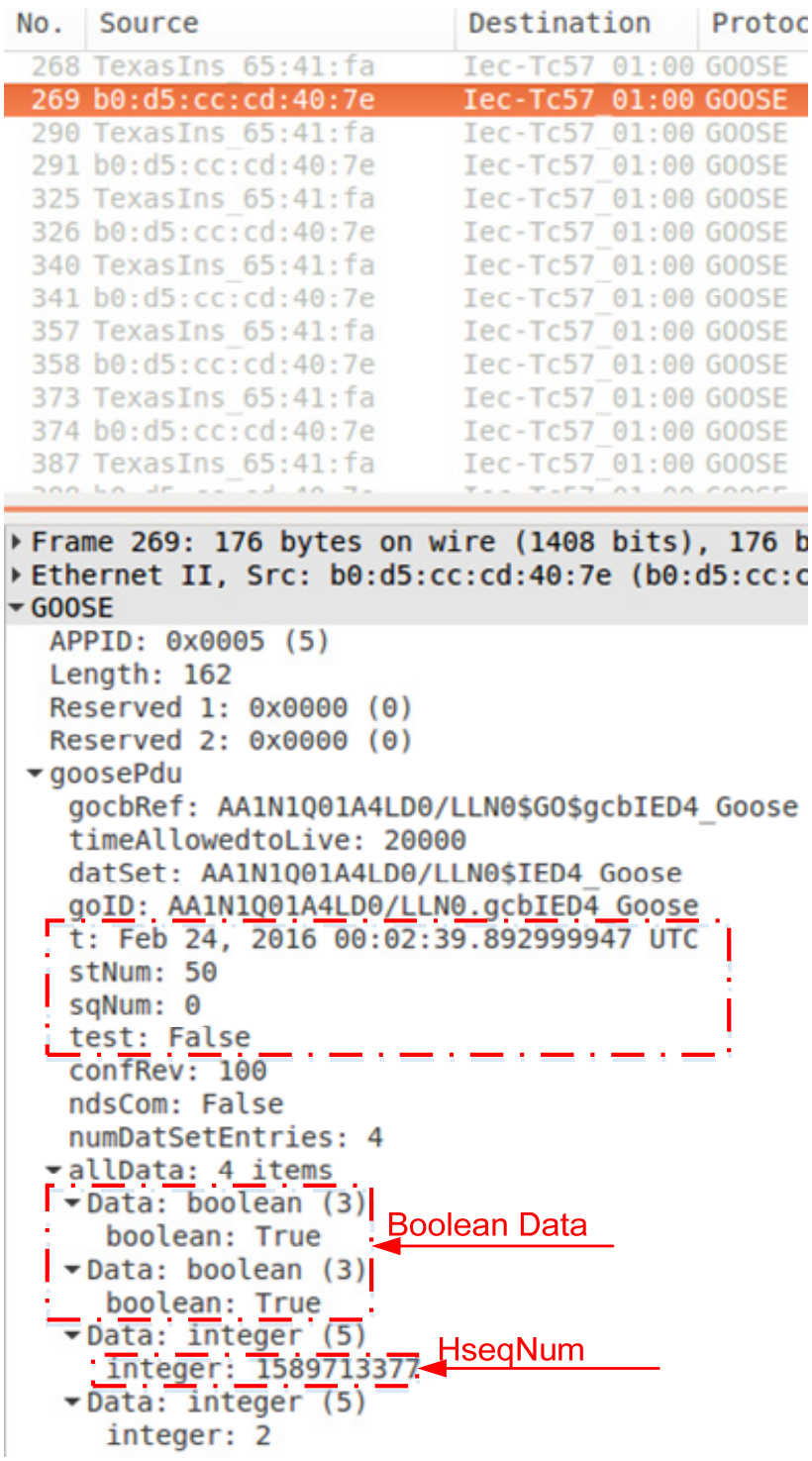


Figure 13.12: GOOSE message with HseqNum field

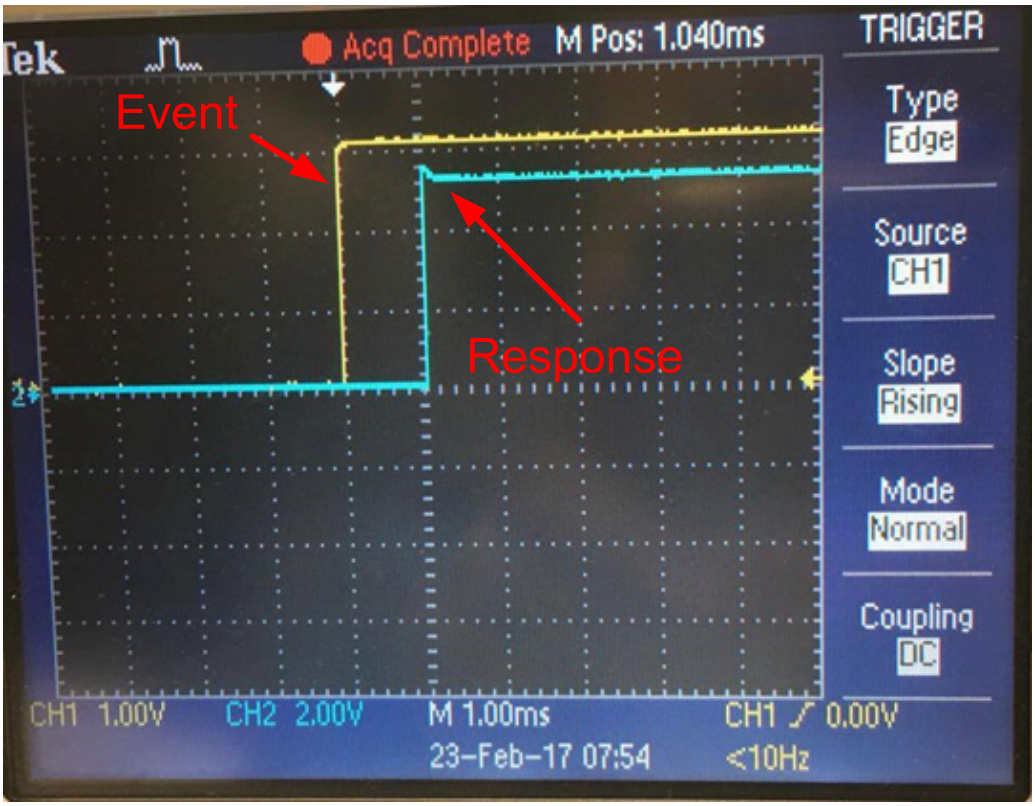


Figure 13.13: Bump in the wire solution end-to-end delay

A GOOSE poisoning and data manipulation attack were performed to test the implemented algorithm. The Sequence hopping algorithm succeeds to discard fake and repeated messages.

13.5 Summary

In this chapter, a security mechanism that addresses the shortcomings in the IEC61850 and IEC 62351 is developed and implemented. The security algorithm protects the IEC 61850 Layer 2 GOSSE messages by preventing message manipulations and GOOSE poisoning attacks by utilizing random sequence hopping number validation. The sequence hopping message validation technique requires minimum processor resources and time. This allows securing the GOOSE message while meeting the 4 ms time

restriction. The end-to-end time delay for the implemented security algorithm is 250 μs for embedded implementation and 1ms for a bump in the wire implementation. The implemented MSSMS server utilizes an SSL encryption channel to synchronize the GOOSE publishers and subscriber. The encryption process doesn't impact the GOOSE message delay since it is used during PRNG synchronization only. In addition, the MSSMS implement algorithm validates the message content with physical rules and policies.

Chapter 14 Conclusions and Recommendation for Future Work

14.1 Conclusions

The co-design of the smart grid as a complex cyber-physical system is demonstrated in this dissertation through the design of a cyber-physical infrastructure for the microgrid. The message-centric and data-centric communication paradigms were analyzed. A comparison between both approaches showed that message-centric communications are not easily expandable, as required by the dynamic nature of the smart grid. A common data bus was implemented based on the data-centric communication approach to provide an efficient, scalable and interoperable communication infrastructure for the microgrid. The data models, along with the necessary QoS profiles for different types of the control signal, are defined. The developed infrastructure was implemented and tested in the smart grid testbed.

An AMI with flexible communication interfaces that allow connections with ZigBee, wifi, and powerline communication networks was developed and integrated with the smart grid testbed. The developed AMI allows modification, implementations and testing new algorithms and ideas for seamless integration with the developed communication infrastructure. Along with the AMI, a high-resolution synchronized measurement network for the distribution network was developed. The reliability and resiliency of this network are improved by utilizing the publisher-subscriber peer-to-peer communication scheme, which eliminates the message broker and single point of failure. This was facilitated by the use of the DDS backbone with proper QoS profile that eliminates the need for phasor data concentrators.

For accurate testing and emulation of the developed smart grid infrastructure, a test bed consisting of a set of modeling and simulation tools representing a scalable HIL infrastructure for a smart grid testbed was developed. The developed infrastructure provides the capability of integrating different types of systems and components inside the testbed and connecting several testbeds to study the behavior of the complex cyber-physical system. A Matlab toolbox was developed to allow integration with modeling software, remote monitoring, and control through a computer network. TLS encryption is used to address security aspect, as well as implementing a routine that checks all remote command against physical rules before passing it to testbed devices.

To improve the microgrid performance by integrating modern communication technology, a synchronization method based on the GPS common time reference for PWM carriers of DC-DC converters is proposed. The proposed technique extends the application of GPS synchronization to the DC microgrid to allow the operation of distributed DC-DC converters modulators as one interleaved converter. The interleave operation of the multiple converters improves the power quality without increasing the size of passive element filters or the switching frequency.

Since the GPS signal is prone to jamming, spoofing and blocking, sensitive systems should have a backup or alternative synchronization method to prevent degradation of system performance. Therefore, a synchronization and PSCA for PWM carriers of DC-DC converters based on carrier extraction was implemented as a backup converter synchronization algorithm.

The main goal of distributed microgrid architecture is to allow efficient integration of renewable resources and to ensure continuity of service to the end user. One of the main factors to maintain stable operation of the microgrid is the synchronization algorithm with utility. For that, an improved adaptive synchronous reference frame phase locked loop ASRF-PLL with islanding detection was developed. This technique shows an excellent performance under unbalanced and distorted voltage conditions. Additionally, to maintain continuous service without interruption in case of islanding, a reconfigurable inverter control was developed to maintain stable operation in the grid connection and stand-alone operation modes of the microgrid. The proposed method ensures islanding detection and stable operation of microgrid when remote islanding detection and the SCADA system fails.

After developing the communication and physical infrastructure for the microgrid, an application layer representing the energy management system is developed. The application layer utilizes the previously discussed communication infrastructure, AMI, and measurement network to efficiently control the microgrids. The developed energy management system has an online optimization module accounting for history, current, and future system observations. Artificial intelligence techniques were utilized to forecast future data related to customer behavior and energy availability. The online optimization adapt the controller's parameters according to change in the customer behavior and energy availability. A hybrid exploration simulation framework was developed to test the efficiency of the optimized parameters before applying them to the real system.

The system security and customer privacy are addressed in the design in both cyber and physical layers. The physical design takes into account the failure of the communication signal, as in the case of the redundant DC-DC converters synchronization and islanding detection. The customer privacy is also addressed in the physical design by implementing a synchronous reference frame-based active power filter controller to compensate for current signature, in addition to different power quality issues for both balanced and unbalanced non-linear loads. The developed controller automatically changes the load current signature, which improves the customer privacy by deceiving NILM.

To address the security and privacy concern that arises from remote identification of electromagnetic signature for certain types of power systems, such as shipboard power system, an HSC was developed to reduce the radiated stray field from heavy current power system components, such as propulsion motors. The developed controller operates online and doesn't need any modification on the physical system design.

Security issues were also addressed on the cyber level. A security analysis and investigation of the IEC 61850 substation automation protocol and IEC 62351 security standard was performed. This study revealed several security shortcomings in the standard. A sequence hopping security mechanism was developed to address revealed shortcoming in the IEC 61850 and IEC 62351 standards. The developed algorithm protects the GOOSE message from message manipulation and GOOSE poisoning attacks. to provide the protection for new and legacy devices, the security mechanism is

implemented as embedded and bump in the wire solution. Both solutions meet the time 4 ms time restriction by introducing time delay 250 μs and 1ms, respectively.

14.2 Recommendations for Future Works

The co-design idea covered in this dissertation address the challenge of designing the smart grid as an integrated cyber-physical system. Several issues related to the system modeling, scalability, interoperability and security are covered in this work. However, due to the complex architecture and multidisciplinary nature of the system, it is recommended that the following topics be expanded by others:

- Data modeling and interoperability: currently there are two main data modeling standards for the power system network, the common information model and the IEC 61850. The common information model covers the transmission and generation area, while the IEC 61850 covers substation automation system. There is a need for a unified data model the covers microgrids and distribution networks. This unified data model should be expanded to cover new technologies and services, such as energy storage, electric vehicles charging stations, vehicles to grid and grid to vehicles services.
- PMU and big data analytic: extending the communication network and PMU application to the active distribution network produces a huge amount of data with a high sampling rate. Processing this huge amount of data in real time to extract useful information to improve the system stability is a big challenge.

There is an urgent need for intelligent and parallel processing techniques to leverage the available data resources.

- Security: the dissertation proposed the sequence hopping security algorithm to secure the IEC 61850 Layer 2 messages. This security mechanism could be expanded to a multi-agent framework, where the agents propagate the alarms and information to the neighbor area for better situational awareness and decision.
- Attack and anomaly detection: an artificial intelligent technique could be integrated with the proposed MSSMS server to detect bad and fake data injection. The intelligent techniques can validate received measurement by learning the physical system's behavior and dynamics, and comparing measured data with previously learned behavior.

References

[1] H. Jiang, Y. Zhang, J. J. Zhang, D. W. Gao and E. Muljadi, "Synchrophasor-Based Auxiliary Controller to Enhance the Voltage Stability of a Distribution System With High Renewable Energy Penetration," in IEEE Transactions on Smart Grid, vol. 6, no. 4, pp. 2107-2115, July 2015

[2] E. Lannoye, "Renewable energy integration: practical management of variability, uncertainty, and flexibility in power grids [book reviews]," in IEEE Power and Energy Magazine, vol. 13, no. 6, pp. 106-107, Nov.-Dec. 2015.

[3] E. B. Ssekulima, M. B. Anwar, A. Al Hinai and M. S. El Moursi, "Wind speed and solar irradiance forecasting techniques for enhanced renewable energy integration with the grid: a review," in IET Renewable Power Generation, vol. 10, no. 7, pp. 885-989, 7 2016.

[4] J. Byun, I. Hong, B. Kang and S. Park, "A smart energy distribution and management system for renewable energy distribution and context-aware services based on user patterns and load forecasting," in IEEE Transactions on Consumer Electronics, vol. 57, no. 2, pp. 436-444, May 2011.

[5] D. Sáez, F. Ávila, D. Olivares, C. Cañizares and L. Marín, "Fuzzy Prediction Interval Models for Forecasting Renewable Resources and Loads in Microgrids," in IEEE Transactions on Smart Grid, vol. 6, no. 2, pp. 548-556, March 2015.

[6] Q. Yang, J. A. Barria and T. C. Green, "Communication Infrastructures for Distributed Control of Power Distribution Networks," in IEEE Transactions on Industrial Informatics, vol. 7, no. 2, pp. 316-327, May 2011.

[7] A. Abdrabou, "A Wireless Communication Architecture for Smart Grid Distribution Networks," in IEEE Systems Journal, vol. 10, no. 1, pp. 251-261, March 2016.

[8] T. Morstyn; B. Hredzak; V. G. Agelidis, "Control Strategies for Microgrids with Distributed Energy Storage Systems: An Overview," in IEEE Transactions on Smart Grid, vol. PP, no.99, pp.1-1, December 2016.

[9] X. Yu and Y. Xue, "Smart Grids: A Cyber–Physical Systems Perspective," in Proceedings of the IEEE, vol. 104, no. 5, pp. 1058-1070, May 2016.

[10] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," in IET Cyber-Physical Systems: Theory & Applications, vol. 1, no. 1, pp. 13-27, 12 2016.

[11] J. Liu, Y. Xiao, S. Li, W. Liang and C. L. P. Chen, "Cyber Security and Privacy Issues in Smart Grids," in IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 981-997, Fourth Quarter 2012.

[12] R. Mahmud, R. Vallakati, A. Mukherjee, P. Ranganathan and A. Nejadpak, "A survey on smart grid metering infrastructures: Threats and solutions," 2015 IEEE International Conference on Electro/Information Technology (EIT), Dekalb, IL, 2015, pp. 386-391.

[13] Chai Jiwen and Liu Shanmei, "Cyber security vulnerability assessment for Smart substations," 2016 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), pp. 1368-1373, Xi'an, 2016.

[14] H. H. Safa, D. M. Souran, M. Ghasempour and A. Khazaee, "Cyber security of smart grid and SCADA systems, threats and risks," CIRED Workshop 2016, pp. 1-4,Helsinki, 2016.

[15] Eric D. Knapp, Raj Samani, "Applied Cyber Security and the Smart Grid", ELSEVIER, 2013, ISBN: 978-1-59749-998-9

[16] J. Zhu, "Communication network for smart grid interoperability," 2015 IEEE International Conference on Communication Software and Networks (ICCSN), pp. 260-265, Chengdu, 2015.

[17] IEEE Draft Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), and End-Use Applications and Loads," in IEEE P2030/D7.0, July 2011, vol., no., pp.1-121, Aug. 2 2011.

[18] Y. Wang, T. T. Gamage and C. H. Hauser, "Security Implications of Transport Layer Protocols in Power Grid Synchrophasor Data Communication," in IEEE Transactions on Smart Grid, vol. 7, no. 2, pp. 807-816, March 2016.

[19] R. Khan, K. McLaughlin, D. Laverty and S. Sezer, "Analysis of IEEE C37.118 and IEC 61850-90-5 synchrophasor communication frameworks," 2016 IEEE Power and Energy Society General Meeting (PESGM, pp. 1-5), Boston, MA, 2016.

[20] N. Kush, E. Ahmed, M. Branagan, E. Foo, "Poisoned GOOSE: Exploiting the GOOSE Protocol", Proceedings of the Twelfth Australasian Information Security Conference-Volume 149, vol. 149, pp. 17-22, 2014.

[21] J. Sigholm and E. Larsson, "Determining the Utility of Cyber Vulnerability Implantation: The Heartbleed Bug as a Cyber Operation," 2014 IEEE Military Communications Conference, pp. 110-116, Baltimore, MD, 2014.

[22] B. Grubb, "Heartbleed disclosure timeline," The Sydney Morning Herald, April 15, 2014 [Online]. Available: http://www. smh. com. au/itpro/ security-it/heartbleed-disclosure-timeline-who-knew-what-andwhen-20140415-zqurk. html.

[23] André N. Albagli, Djalma M. Falcão, José F. de Rezende, "Smart grid framework co-simulation using HLA architecture," Electric Power Systems Research, Volume 130, January 2016, Pages 22-33, ISSN 0378-7796.

[24] Dhananjay Bhor, Kavinkadhirselvan Angappan, Krishna M. Sivalingam, "Network and power-grid co-simulation framework for Smart Grid wide-area monitoring networks," Journal of Network and Computer Applications, Volume 59, Pages 274-284 January 2016.

[25] G. Celli, P. A. Pegoraro, F. Pilo, G. Pisano and S. Sulis, "DMS Cyber-Physical Simulation for Assessing the Impact of State Estimation and Communication Media

in Smart Grid Operation," in IEEE Transactions on Power Systems, vol. 29, no. 5, pp. 2436-2446, Sept. 2014.

[26] E. Sharma, C. Chiculita and Y. Besanger, "Co-simulation of a low-voltage utility grid controlled over IEC 61850 protocol," 2015 5th International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT), Changsha, 2015, pp. 2365-2372.

[27] Oh, S.-J.; Yoo, C.-H.; Chung, I.-Y.; Won, D.-J."Hardware-in-the-Loop Simulation of Distributed Intelligent Energy Management System for Microgrids," Energies 2013, 6, 3263-3283.

[28] M. S. Almas and L. Vanfretti, "RT-HIL Implementation of the Hybrid Synchrophasor and GOOSE-Based Passive Islanding Schemes," in IEEE Transactions on Power Delivery, vol. 31, no. 3, pp. 1299-1309, June 2016.

[29] David Goughnour, Joe Stevents, "Testing Intelligent Device Communications in Distributed System," Available Online: http://trianglemicroworks.com/docs/default-source/referenced-documents/testing-intelligent-device-communications-in-a-distributed-system.pdf?sfvrsn=2 (Accessed on 01/04/2017).

[30] Ravi Akella, Han Tang, Bruce M. McMillin, "Analysis of information flow security in cyber–physical systems," International Journal of Critical Infrastructure Protection, Volume 3, Issues 3–4, December 2010, Pages 157-173, ISSN 1874-5482.

[31] Ahmed, M.A.; Kang, Y.C.; Kim, Y.-C. "Communication Network Architectures for Smart-House with Renewable Energy Resources," Energies 2015, 8, 8716–8735.

[32] Huang, J.F.; Wang, H.G.; Qian, Y. "Smart grid communications in challenging environments," In Proceedings of the 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), Tainan, Taiwan, 5–8 November 2012; pp. 552–557.

[33] Martínez, J.-F.; Rodríguez-Molina, J.; Castillejo, P.; De Diego, R. "Middleware Architectures for the Smart Grid: Survey and Challenges in the Foreseeable Future," Energies 2013, 6, 3593–3621.

[34] Ardito, L.; Procaccianti, G.; Menga, G.; Morisio, M., "Smart Grid Technologies in Europe: An Overview," Energies 2013, 6, 251–281.

[35] Hahn, A.; Ashok, A.; Sridhar, S.; Govindarasu, M. "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," IEEE Trans. Smart Grid 2013, 4, 847–855.

[36] The Smart Grid: An Introduction, US Department of Energy. Available online: http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages(1).pdf (accessed on 25 February 2016).

[37] Ozansoy, C.R.; Zayegh, A.; Kalam, A. "The real-time publisher/subscriber communication model for distributed substation systems," IEEE Trans. Power Deliv. 2007, 22, 1411–1423.

[38] Zaballos, A.; Vallejo, A.; Selga, J.M., “Heterogeneous communication architecture for the smart grid,” IEEE Netw. 2011, 25, 30–37.

[39] Schlesselman, J.M.; Pardo-Castellote, G.; Farabaugh, B. “OMG data-distribution service (DDS): Architectural update,” In Proceedings of the 2004 IEEE Military Communications Conference, MILCOM 2004, Monterey, CA, USA, 31 October–3 November 2004; Volume 2, pp. 961–967.

[40] De Diego, R.; Martínez, J.-F.; Rodríguez-Molina, J.; Cuerva, A. “A Semantic Middleware Architecture Focused on Data and Heterogeneity Management within the Smart Grid,” Energies 2014, 7, 5953–5994.

[41] Komninos, N.; Philippou, E.; Pitsillides, A. “Survey in smart grid and smart home security: Issues, challenges and countermeasures,” IEEE Commun. Surv. Tutor. 2014, 16, 1933–1954.

[42] RTI Whitepaper, Data Centric Middleware. Available online: http://www.rti.com/docs/RTI_Data_Centric_Middleware.pdf (accessed on 25 February 2016).

[43] El Hariri, Mohamad; Youssef, Tarek A.; Mohammed, Osama A. 2016. "On the Implementation of the IEC 61850 Standard: Will Different Manufacturer Devices Behave Similarly under Identical Conditions?" Electronics 5, no. 4: 85.

[44] Schmidt, D.C.; Van’t Hag, H. “Addressing the challenges of mission-critical information management in next-generation net-centric pub/sub systems with opensplice DDS,” In Proceedings of the IEEE International Symposium on Parallel and Distributed Processing (IPDPS), Miami, FL, USA, 14–18 April 2008; pp. 1–8.

[45] Data Distribution Service for Real-time Systems; Version 1.2; Available Online https://community.rti.com/filedepot_download/1795/16 (accessed on 25 February 2016).

[46] Pardo-Castellote, G. “OMG data distribution service: Architectural overview,” In Proceedings of the Military Communications Conference, Boston, MA, USA, 13–16 October 2003; Volume 1, pp. 242–247.

[47] Esposito, C.; Russo, S.; Di Crescenzo, D. “Performance assessment of OMG compliant data distribution middleware,” In Proceedings of the IEEE International Symposium on Parallel and Distributed Processing, Miami, FL, USA, 14–18 April 2008; pp. 1–8.

[48] Aegis Open Architecture Weapon System. Available online: http://www.rti.com/docs/Lockheed.pdf (accessed on 25 February 2016).

[49] Delivering High-Performance, Scalable and Safe Data Distribution in Next Generation Air Traffic Control and Management. Available online: http://www.prismtech.com/sites/default/files/documents/OpenSplice_DDS_ATC_ATM_Overview.pdf (accessed on 25 February 2016).

[50] Secure, High-Reliability and High-Performance Scalable Infrastructure. Available online: http://www.rti.com/industries/energy.html (accessed on 25 February 2016).

[51] Open Field Message Bus (OpenFMB). Available online: http://members.sgip.org/apps/group_public/download.php/6353/2015-03-05%20OFMB%20Kickoff%20Presentation%20DRAFT.pptx (accessed on 10/05/2015).

[52] The Real-Time Publish-Subscribe Wire Protocol DDS Interoperability Wire Protocol Specification; Object Management Group: Needham, USA, 2009.

[53] Gerardo P.C., "Data Distribution Service A Foundation of Real-Time Data Centricity". Available Online:http://omgwiki.org/dds/sites/default/files/dds_06-09-04.pdf (Accessed on 01/25/2017)

[54] Salehi, V.; Mohamed, A.; Mazloomzadeh, A.; Mohammed, O.A. "Laboratory-based smart power system, part I: Design and system development," IEEE Trans. Smart Grid 2012, 3, 1394–1404.

[55] Amin, M.M.; Mohammed, O.A. "Development of high-performance grid-connected wind energy conversion system for optimum utilization of variable speed wind turbines," IEEE Trans. Sustain. Energy 2011, 2, 235–245.

[56] Corradi, A.; Foschini, L. A "DDS-compliant P2P infrastructure for reliable and QoS-enabled data dissemination," In Proceedings of the IEEE International Symposium on Parallel & Distributed Processing, Rome, Italy, 23–29 May 2009; pp. 1–8.

[57] Limited-Bandwidth Plug-ing for DDS. Available online: http://www.rti.com/docs/DDS_Over_Low_Bandwidth.pdf (accessed on 25 February 2016).

[58] http://www.st.com/content/ccc/resource/technical/document/datasheet/df/07/5e/81/99/48/4c/57/CD00235593.pdf/files/CD00235593.pdf/jcr:content/translations/en.CD00235593.pdf (last accessed at feb 27 2017)

[59] von Meier, Alexandra, and Reza Arghandeh. "Every Moment Counts: Synchrophasors for Distribution Networks with Variable Resources." arXiv preprint arXiv:1408.1736 (2014).

[60] A. von Meier, D. Culler, A. McEachern and R. Arghandeh, "Micro-synchrophasors for distribution systems," ISGT 2014, pp. 1-5, Washington, DC, 2014.

[61] Emgell, S. Cyber-Physical Systems of Systems—Definition and Core Research and Innovation Areas. Working Paper of the Support Action CPSoS, 26 October 2014. Available online: http://www.cpsos.eu/wp-content/uploads/2015/07/CPSoS-Scope-paper-vOct-26–2014.pdf (accessed on 25 February 2016).

[62] Hossain, E.; Kabalci, E.; Bayindir, R.; Perez, R. "Microgrid testbeds around the world: State of art. Energy Convers," Manag. 2014, 86, 132–153.

[63] Hossain, M.A.; Dasgupta, D.; Abercrombie, R.K. "OPNET/simulink based testbed for disturbance detection in the smart grid," In Proceedings of the 10th Annual Cyber and Information Security Research Conference, Oak Ridge, TN, USA, 7–9 April 2015.

[64] Bhor, D.; Angappan, K.; Sivalingam, K.M. “Network and power-grid co-simulation framework for Smart Grid wide-area monitoring networks,” J. Netw. Comput. Appl. 2016, 59, 274–284.

[65] Huang J, “A review on distributed energy resources and MicroGrid,” Renewable and Sustainable Energy Reviews, vol.12, Page(s): 2472–2483, 2008.

[66] Najy, W.K.A, Zeineldin, H.H., Woon, W.L. “Optimal Protection Coordination for Microgrids With Grid-Connected and Islanded Capability,” IEEE Transaction on industrial electronics, vol. 60, Issue: 4, Page(s): 1668 - 1677, 2013.

[67] Jackson John Justo, “AC-microgrids versus DC-microgrids with distributed energy resources: A review,” Renewable and Sustainable Energy Reviews, vol. 24, Page(s): 387–405, 2013

[68] C. Yoon, J. Kim, and S. Choi, “Multiphase DC–DC converters using a boost-half-bridge cell for high-voltage and high-power applications,” IEEE transaction on power electronics, vol. 26, no. 2, pages(s): 381–388, Feb. 2011

[69] Carrasco, J.M; Franquelo, L.G.; Bialasiewicz, J.T.; Galvan, E. “Power-Electronic Systems for the Grid Integration of Renewable Energy Sources: A Survey,” IEEE transaction on industrial electronics, vol. 53, Issue: 4, Page(s): 1002 - 1016, 2006

[70] Chien-Ming Wang, Chang-Hua Lin, Shih-Yung Hsu, Chien-Min Lu, Jyun-Che Li, “Analysis, design and performance of a zero-currentswitching pulse-width-modulation interleaved boost dc/dc converter,” IET Power Electron., Vol. 7, Iss. 9, pp. 2437–2445, 2014.

[71] M. Elsied, A. Salem, A. Oukaour, H. Gualous, H. Chaoui, T. Youssef, De. Belie, J. Melkebeek, O. Mohammed,’’ Efficient power-electronic converters for electric vehicle applications’’, in: 2015 IEEE Vehicle Power and Propulsion Conference (VPPC), Montreal, 2015.

[72] Kai Zhang, Zhenyu Shan and Juri Jatskevich, Senior Member, IEEE, “Large- and Small-Signal Average-Value Modeling of Dual-Active-Bridge DC–DC Converter Considering Power Losses,” IEEE Trans. Power Electron, Vol. 99, no. 1, pp. 1-1, April. 2016..

[73] DAS. M, Agarwal. V, “Design and Analysis of a High Efficiency DC-DC Converter with Soft Switching Capability for Renewable Energy Applications Requiring High Voltage Gain,” IEEE transaction on industrial electronics, vol. PP, issue. 99, Page(s): 1, 2016.

[74] Yu Gu, and Donglai Zhang, Member, IEEE, “Interleaved Boost Converter with Ripple Cancellation Network”, IEEE Trans. Power Electron, VOL. 28, no. 8, August 2013.

[75] Luo-wei Zhou, Bin-xin Zhu, Quan-ming Luo, Si Chen,’’ Interleaved non-isolated high step-up DC/DC converter based on the diode–capacitor multiplier, IET Power Electron. , Vol. 7, Iss. 2, pp. 390–397, 2014.

[76] A. Salem, M. Elsied, J. Druant, F. De Belie, A.Oukaour, H.Gualous, and J. Melkebeek "An Advanced Multilevel Converter Topology with Reduced Switching Elements,", in: the 40th Annual Conference of the IEEE Industrial Electronics IECON 2014, Dallas, USA, 2014

[77] P. Thounthong and B. Davat, "Study of a multiphase interleaved step-up converter for fuel cell high power applications," Energy Convers. Manag., vol. 51, no. 4, pp. 826–832, 2010.

[78] A. Prodic, D. Maksimovic and R.W. Erickson, "Design and implementation of a digital PWM controller for a high-frequency switching DC-DC power converter," Proc. the 26th Annual Conference of the IEEE Industrial Electronics IECON 2001, pp. 893-898, 2001

[79] Pengfei Li," Synchronization and control of high frequency DC-DC converters", PhD thesis; Florida university,2009.

[80] IEEE Std. 1588-2008. ", IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems'', Available: http://www.nist.gov/el/isd/ieee/ieee1588.cfm [Accessed Feb 28/ 20016].

[81] National Instruments, "Timing and Synchronization Systems," [Online]. Available http://www.ni.com/white-paper/9882/en/ . [Accessed Feb 28/ 2016].

[82] Wenbo Shi, Na Li, Member, and Rajit Gadh; "Real-Time Energy Management in Microgrids" IEEE TRANSACTIONS ON SMART GRID, Vol 99, PP:1-1, August 2015.

[83] Priewasser. R, Agostinelli. M, Unterrieder. C, Marsili. S, "Modeling, Control, and Implementation of DC–DC Converter for Variable Frequency Operation," IEEE Trans. Power Electron, Vol. 29, no. 1, pp. 287–301, Jan. 2014.

[84] https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/faq/gps/ [Accessed Feb 27/ 2017].

[85] Boyr; France Thomas J. L "A review on synchronization methods for grid-connected three-phase VSC under unbalanced and distorted conditions" in Power Electronics and Applications (EPE 2011), Proceedings of the 2011-14th European Conference, pp. 1-10, 2011.

[86] Fainan Hassan and Roger Critchley "A Robust PLL for Grid Interactive Voltage Source Converters" in Power Electronics and Motion Control Conference (EPE/PEMC), 14th International, pp. T2-29-T2-35, 2010.

[87] Fran González-Espí; Emilio Figueres; Gabriel Garcerá "An Adaptive Synchronous-Reference-Frame Phase-Locked Loop for Power Quality Improvement in a Polluted Utility Grid" in Industrial Electronics, IEEE Transactions on, Volume: 59 , Issue: 6, pp. 2718 – 2731, 2012.

[88] Yun-Hyun Kim; Kwang-Seob Kim; Byung-Ki Kwon; Chang-Ho Choi "A fast and robust pll of mcfc pcs under unbalanced grid voltage" in Power Electronics Specialists Conference, PESC 2008. IEEE

[89] Canbing Li, Chi Cao, Yijia Cao, Yonghong Kuang, Long Zeng, Baling Fang, “A review of islanding detection methods for microgrid,” Renewable and Sustainable Energy Reviews, Volume 35, July 2014, Pages 211-220, ISSN 1364-0321, http://dx.doi.org/10.1016/j.rser.2014.04.026.

[90] A. Mazloomzadeh, M. H. Cintuglu and O. A. Mohammed, "Islanding detection using synchronized measurement in smart microgrids," 2013 IEEE PES Conference on Innovative Smart Grid Technologies (ISGT Latin America), Sao Paulo, 2013, pp. 1-7., pp. 4712-4716, 2013.

[91] Ghoshal, Anirban and John, Vinod, “A Method to Improve PLL Performance Under Abnormal Grid Conditions,” In: National Power Electronics Conference, Indian Institute of Science, Bangalore, 2007.

[92] A. Basit, G. A. S. Sidhu, A. Mahmood and F. Gao, "Efficient and Autonomous Energy Management Techniques for the Future Smart Homes," in IEEE Transactions on Smart Grid, vol. 8, no. 2, pp. 917-926, March 2017

[93] C. Zhao; J. He; P. Cheng; J. Chen, "Consensus-Based Energy Management in Smart Grid With Transmission Losses and Directed Communication," in IEEE Transactions on Smart Grid , vol.PP, no.99, pp.1-13, January 2016.

[94] W. Shi, X. Xie, C. C. Chu and R. Gadh, "Distributed Optimal Energy Management in Microgrids," in IEEE Transactions on Smart Grid, vol. 6, no. 3, pp. 1137-1146, May 2015.

[95] S. Salinas, M. Li, P. Li and Y. Fu, "Dynamic Energy Management for the Smart Grid With Distributed Energy Resources," in IEEE Transactions on Smart Grid, vol. 4, no. 4, pp. 2139-2151, Dec. 2013.

[96] Z. Chen and L. Wu, "Residential Appliance DR Energy Management With Electric Privacy Protection by Online Stochastic Optimization," in IEEE Transactions on Smart Grid, vol. 4, no. 4, pp. 1861-1869, Dec. 2013.

[97] OpenEI. Available Online: en.openei.org/datasets/dataset (accessed on March 2015).

[98] Object Management Group (OMG), the Real-time Publish-Subscribe Wire Protocol DDS Interoperability Wire Protocol Specification, 2009.

[99] Assessment of Demand Response and Advanced Metering. Available online: https://www.ferc.gov/legal/staff-reports/2015/demand-response.pdf (accessed on 01 December 2016).

[100] Florida Power and Light Company. Available Online” https://www.fpl.com/rates/pdf/Sept2016-Residential.pdf” (Accessed on 20 November 2016).

[101] D. G. Vutetakis and H. Wu, "The effect of charge rate and depth of discharge on the cycle life of sealed lead-acid aircraft batteries," IEEE 35th International Power Sources Symposium, pp. 103-105, Cherry Hill, NJ, 1992.

[102] Y. Gong, Y. Cai, Y. Guo and Y. Fang, "A Privacy-Preserving Scheme for Incentive-Based Demand Response in the Smart Grid," in IEEE Transactions on Smart Grid, vol. 7, no. 3, pp. 1304-1313, May 2016.

[103] M. Zeifman and K. Roth, "Nonintrusive appliance load monitoring: Review and outlook," in IEEE Transactions on Consumer Electronics, vol. 57, no. 1, pp. 76-84, February 2011.

[104] G. W. Hart, "Nonintrusive appliance load monitoring," in Proceedings of the IEEE, vol. 80, no. 12, pp. 1870-1891, Dec 1992.

[105] H. H. Chang, K. L. Chen, Y. P. Tsai and W. J. Lee, "A New Measurement Method for Power Signatures of Nonintrusive Demand Monitoring and Load Identification," in IEEE Transactions on Industry Applications, vol. 48, no. 2, pp. 764-771, March-April 2011.

[106] C. Dinesh, B. W. Nettasinghe, R. I. Godaliyadda, M. P. B. Ekanayake, J. Ekanayake and J. V. Wijayakulasooriya, "Residential Appliance Identification Based on Spectral Information of Low Frequency Smart Meter Measurements," in IEEE Transactions on Smart Grid, vol. 7, no. 6, pp. 2781-2792, Nov. 2016.

[107] Timothy John Eastham, Reactive Power Control in Electric Systems, Wiley, 1982.

[108] Leon M. Tolbert, Harold D. Hollis and Peyton S. Hale, "Evaluation of Harmonic Suppression Devices", IEEE Thirty-First IAS Annual Meeting, San Diego, CA, PP. 2340-2346, Oct. 1996.

[109] Ali I. and M. H. Haque, "Harmonics, Sources, Effects and Mitigation Techniques", Second International conference on Electrical and Computer Engineering (ICECE), PP. 87-90, December 2002.

[110] Illindala, M.; Venkataramanan, G., "Frequency/Sequence Selective Filters for Power Quality Improvement in a Microgrid," Smart Grid, IEEE Transactions on , vol.3, no.4, pp.2039,2047, Dec. 2012.

[111] Corasaniti, V.F.; Barbieri, M.B.; Arnera, P.L., "Compensation with Hybrid Active Power Filter in an Industrial Plant," Latin America Transactions, IEEE (Revista IEEE America Latina) , vol.11, no.1, pp.447,452, Feb. 2013.

[112] Bhattacharya, A.; Chakraborty, C.; Bhattacharya, S., "Parallel-Connected Shunt Hybrid Active Power Filters Operating at Different Switching Frequencies for Improved Performance," Industrial Electronics, IEEE Transactions on , vol.59, no.11, pp.4007,4019, Nov. 2012.

[113] Acuna, P.; Moran, L.; Rivera, M.; Dixon, J.; Rodriguez, J., "Improved Active Power Filter Performance for Renewable Power Generation Systems," Power Electronics, IEEE Transactions on , vol.29, no.2, pp.687,694, Feb. 2014.

[114] Round S.D. and Ingram D.M.E, " An Evaluation of Techniques for Determining Active Filter Compensating Currents in Unbalanced Systems", Proc. Of the European Conf. on Power Electronics and Applications, Vol. 4, no. 5, PP. 767-772, Trondheim, 1997.

[115] H. Akagi, E. H. Watanabe and M. Aredes, “Instantaneous Power Theory to Power Conditioning,” Wiley, 2007.

[116] H. Akagi, E. H. Watanabe and M. Aredes, " More power to you (review of Instantaneous Power Theory to Power Conditioning by Akagi, H. et al.; 2007)", IEEE Power and Energy Magazine, Vol. 6, no. 1, PP. 80-81, 2008.

[117] Bhim Singh , Kamal Al-Haddad and Ambrish Chandra, "A Review of Active filters for Power Quality Improvement", IEEE Trans. on Industrial Electronics , Vol. 46, no. 5, PP. 960-967, Oct. 1999.

[118] Tarek Youssef and O. A. Mohammed, " Adaptive SRF-PLL with Reconfigurable Controller for Microgrid in Grid-Connected and Stand-Alone Modes" 2013 Power and Energy Society General Meeting, Vancouver, B.C., Canada, 21-25 Jul 2013.

[119] Simone Buso, Luigi Malesani and Paolo Mattavelli, "Comparison of Current Control Techniques for Active filter Applications", IEEE Trans. on Industrial Electronics , Vol. 45, no. 5, PP. 722-729, Oct. 1998.

[120] Ingram D.M.E. and Round S.D, " A Novel Digital Hysteresis Current Controller for an Active Power Filter", Proc. of Conf. on Power Electronics and Drive Systems, vol. 2, pp. 744-749, Singapore, 1999.

[121] J.-F. Brudny and J.-P. Lecointe, “Rotor design for reducing the switching magnetic noise of AC electrical machine variable-speed drives,” IEEE Trans. Ind. Electron., vol. 58, no. 11, pp. 5112–5120, Nov. 2011.

[122] R. Islam, I. Husain, A. Fardoun, and K. McLaughlin, “Permanent magnet synchronous motor magnet designs with skewing for torque ripple and cogging torque reduction,” IEEE Trans. Ind. Appl., vol. 45, no. 1, pp. 152–160, Jan./Feb. 2009.

[123] Y. Liu, Z. Q. Zhu, and D. Howe, “Direct torque control of brushless DC drives with reduced torque ripple,” IEEE Trans. Ind. Appl., vol. 41, no. 2, pp. 599–608, Mar./Apr. 2005.

[124]] Z. Zhengming et al., “Hybrid selective harmonic elimination PWM for common-mode voltage reduction in three-level neutral-point-clamped inverters for variable speed induction drives,” IEEE Trans. Power Electron., vol. 27, no. 3, pp. 1152–1158, Mar. 2012.

[125] B. Ozpineci, L. M. Tolbert, and J. N. Chiasson, “Harmonic optimization of multilevel converters using genetic algorithms,” in Proc. IEEE 35th Annu. Power Electron. Spec. Conf., vol. 5, 2004, pp. 3911–3916.

[126] W. Fei, X. Ruan, and B. Wu, “A generalized formulation of quarter-wave symmetry SHE-PWM problems for multilevel inverters,” IEEE Trans. Power Electron., vol. 24, no. 7, pp. 1758–1766, Jul. 2009

[127] M. S. A. Dahidah and V. G. Agelidis, “Selective harmonic elimination PWM control for cascaded multilevel voltage source converters: A generalized formula,” IEEE Trans. Power Electron., vol. 23, no. 4, pp. 1620–1630, Jul. 2008.

[128] E. Babaei, S. H. Hosseini, and G. B. Gharehpetian, "Reduction of THD and low order harmonics with symmetrical output current for single-phase ac/ac matrix converters," Int. J. Elect. Power Energy Syst., vol. 32, no. 3, pp. 225–235, Mar. 2010.

[129] Z. Du, L. M. Tolbert, and J. N. Chiasson, "Active harmonic elimination for multilevel converters," IEEE Trans. Power Electron., vol. 21, no. 2, pp. 459–469, Mar. 2006.

[130] Z. Du, L. M. Tolbert, and J. N. Chiasson, "Active harmonic elimination in multilevel converters using FPGA control," in Proc. IEEE Workshop Comput. Power Electron., Urbana-Champaign, IL, USA, Aug. 2004, pp. 127–132.

[131] Z. Du, L.M. Tolbert, and J. N. Chiasson, "Harmonic elimination in multilevel converter with programmed PWMmethod," in Proc. IEEE Ind. Appl. Soc. Annu. Meeting, Seattle, WA, USA, Oct. 2004, pp. 2210–2215.

[132] V. G. Agelidis, A. Balouktsis, I. Balouktsis, and C. Cossar, "Five-level selective harmonic elimination PWM strategies and multicarrier phase shifted sinusoidal PWM: A comparison," in Proc. IEEE Power Electron. Spec. Conf., Recife, Brazil, Jun. 2005, pp. 1685–1691.

[133] V. G. Agelidis, A. Balouktsis, and M. S. A. Dahidah, "A five-level symmetrically defined selective harmonic elimination PWM strategy: Analysis and experimental validation," IEEE Trans. Power Electron., vol. 23, no. 1, pp. 19–26, Jan. 2008.

[134] M. S. A. Dahidah and V. G. Agelidis, "Generalized formulation of multilevel selective harmonic elimination PWM: Case I—Non-equal dc sources," in Proc. IEEE Power Electron. Spec. Conf., Jeju, Korea, Jun. 2006, pp. 472–1477.

[135] H. A. Toliyat et al., "Electric Machines: Modeling, Condition Monitoring, and Fault Diagnosis," Boca Raton, FL, USA: CRC Press, 2012.

[136] M. Barzegaran, A. Mazloomzadeh, and O. A. Mohammed, "Fault diagnosis of the asynchronous machines through magnetic signature analysis using finite-element method and neural networks," IEEE Trans. Energy Convers., vol. 28, no. 4, pp. 1064–1071, Dec. 2013.

[137] C. Lascu et al., "High performance current controller for selective harmonic compensation in active power filters," IEEE Trans. Power Electron., vol. 22, no. 5, pp. 1826–1835, Sep. 2007.

[138] F. Z. Peng, J.-S. Lai, J.W. McKeever, and J. VanCoevering, "A multilevel voltage-source inverter with separateDCsources for static var generation,"IEEE Trans. Ind. Appl., vol. 32, no. 5, pp. 1130–1138, Sep./Oct. 1996.

[139] J. Rodriguez, J. S. Lai, and F. Z. Peng, "Multilevel inverters: A survey of topologies, controls, and applications," IEEE Trans. Ind. Electron., vol. 49, no. 4, pp. 724–738, Aug. 2002.

[140] A. Kavousi, B. Vahidi, R. Salehi, M. Bakhshizadeh, N. Farokhnia, and S. S. Fathi, "Application of the bee algorithm for selective harmonic elimination strategy in

multilevel inverters," IEEE Trans. Power Electron., vol. 27, no. 4, pp. 1689–1696, Apr. 2012.

[141] S. B. A. Khalid, G. Aliyu, M. W. Mustafa, and H. Shareef, "An improved Walsh function algorithm for use in sinusoidal and nonsinusoidal power components measurement," J. Energy, vol. 2013, art. no. 807639, p. 10, 2013.

[142] Y. Liu, H. Hong, and A. Q. Huang, "Real-time calculation of switching angles minimizing THD for multilevel inverters with step modulation," IEEE Trans. Ind. Electron., vol. 56, no. 2, pp. 285–293, Feb. 2009.

[143] K. Georgakas, P. Vovos, and N. Vovos, "Harmonic reduction method for a single-phase dc-ac converter without output filter," IEEE Trans. Power Electron., vol. 29, no. 9, pp. 4624–4632, Sep. 2013.

[144] S. Jeevananthan, R. Nandhakumar, and P. Dananjayan, "Inverted sine carrier for fundamental fortification in PWM inverters and FPGA based implementations," Serbian J. Elect. Eng., vol. 4, no. 2, pp. 171–187, 2007.

[145] J. R. Rodr´ıguez et al., "PWM regenerative rectifiers: State of the art," IEEE Trans. Ind. Electron., vol. 52, no. 1, pp. 5–22, Feb. 2005.

[146] A. Radan, A. H. Shahirinia, and M. Falahi, "Evaluation of carrier-based PWM methods for multi-level inverters," in Proc. IEEE Int. Symp. Ind. Electron., 2007, pp. 389–394.

[147] M. Barzegaran, A. Mohamed, T. Youssef, and O. A. Mohammed, "Electromagnetic signature study of a power converter connected to an electric motor drive," IEEE Trans. Magn., vol. 50, no. 2, pp. 201–204, Feb. 2014.

[148] J. W. Gordon and J. O. Smith, "A Sine Generation Algorithm for VLSI Applications," in Proc. Int. Computer Music Conf. (1985), pp. 165–168.

[149]] V. F. Kroupa, "Direct Digital Frequency Synthesizers," Piscataway, NJ, USA: IEEE Press, 1999.

[150] P. C. Krause et al., "Analysis of Electric Machinery and Drive Systems", vol. 75. Hoboken, NJ, USA: Wiley, 2013.

[151] J. A. Baroudi, V. Dinavahi, and A. M. Knight, "A review of power converter topologies for wind generators," Renewable Energy, vol. 32, no. 14, pp. 2369–2385, Nov. 2007.

[152] S. K. Mondal et al., "Space vector pulse width modulation of three-level inverter extending operation into overmodulation region," IEEE Trans. Power Electron., vol. 18, no. 2, pp. 604–611, Mar. 2003.

[153] Technical Report "IEC TR 61850-1", First edition, 2003-04, reference number IEC/TR 61850-1:2003(E)

[154] J. Hoyos, M. Dehus, and T. X. Brown, "Exploiting the goose protocol: A practical attack on cyber-infrastructure," in Globecom Workshops (GC Wkshps), 2012 IEEE. IEEE, 2012, pp. 1508–1513.

[155] M. T. A. Rashid, S. Yussof, Y. Yusoff, and R. Ismail, “A review of security attacks on iec61850 substation automation system network,” in Information Technology and Multimedia (ICIMU), 2014 International Conference on. IEEE, 2014, pp. 5–10.

[156] M. Hariri, T. Youssef, and O.A. Mohammed, “On the Implementation of IEC 61850 Standard: Will Different Manufacturer Devices Behave Similarly Under Identical Condistions?”. Electronics, 2016.

[157] Q. Li, C. Ross, J. Yang, J. Di, J. C. Balda, and H. A. Mantooth, “The effects of flooding attacks on time-critical communications in the smart grid.”

[158] N Kush, E. Ahmed, M. Branagan, Ernest .F, " Poisoned GOOSE: Exploiting the GOOSE Protocol," Proceedings of the Twelfth Australasian Information Security Conference (AISC 2014), Auckland, New Zealand, pp. 17-22.

[159] H. Falk, “Securing iec 61850,” in 2008 IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008.

[160] Frances Cleveland “IEC 62351 Security Standards for the Power system Information Infrastructure”. IEC TC57 WG15 security standard Ver 14, June, 2012.

[161] E. D. Knapp, “Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure” Elsevier, 2013.

[162] F. Hohlbaum, M. Braendle, and F. Alvarez, “Cyber security practical considerations for implementing iec 62351,” Switzerland, library.e.abb.com.

[163] S. Fuloria, R. Anderson, K McGrath, K Hansen, F Alvarez, “The Protection of Substation Communications”, ABB Corporate research, https://www.cl.cam.ac.uk/~rja14/Papers/S4-2010.pdf.

VITA

TAREK YOUSSEF

1977	Born, Cairo, Egypt
1996-2001	B.S., Electrical Engineering Helwan University, Cairo, Egypt
2008	M.S., Electrical Engineering Helwan University, Cairo, Egypt
2012-2017	Doctoral Candidate, Electrical Engineering
2015	Outstanding Scholar award for Academic Achievement and Academic Research, Florida International University
2017	Award, Dissertation Year Fellowship Florida International University, Miami, Florida

SELECTED PUBLICATIONS AND PRESENTATIONS

[1] Tarek A. Youssef, Ahmed T. Elsayed, Osama A. Mohammed "data distribution service based Interoperability Framework for Smart Grid Testbed Infrastructure", Energies Journal, 2 March 2016.

[2] M. H. Cintuglu; T. Youssef; O. A. Mohammed, "Development and Application of a Real-Time Testbed for Multiagent System Interoperability: A Case Study on Hierarchical Microgrid Control," in IEEE Transactions on Smart Grid , vol.PP, no.99, pp.1-1.

[3] El Hariri Mohamad, Tarek A. Youssef, and Osama A. Mohammed. "On the Implementation of the IEC 61850 Standard: Will Different Manufacturer Devices Behave Similarly under Identical Conditions?" Electronics 5.4 (2016): 85.

[4] H. F. Habib, T. Youssef, M. H. Cintuglu and O. Mohammed, "A multi-agent based technique for fault location, isolation and service restoration," 2016 IEEE Industry Applications Society Annual Meeting, Portland, OR, 2016, pp. 1-8.

[5] M.R Barzegaran, Ahmed Mohamed, Tarek Youssef, O.A. Mohammed "Electromagnetic signature study of the power converter connected to an electric motor drives," IEEE Transaction on Magnetics (Volume:50 , Issue: 2), Feb. 2014.

[6] M. R. Barzegaran, Tarek Youssef, Alberto Berzoy, , O. A Mohammed, "Electric

Machine Drive Design Improvements through Control and Digital Signal Processing Techniques", Accepted for IEEE Transaction on Energy conversion.

[7] Abla O. Hariri, Tarek Youssef, Ahmed T. Elsayed, Osama Mohammed, "A Computational Approach for a Wireless Power Transfer Link Design Optimization Considering Electromagnetic Compatibility", Accepted to be published in IEEE Transactions on Magnetics. DOI: 10.1109/TMAG.2015.2492922.

[8] A. T. Elsayed, T. A. Youssef and O. A. Mohammed, "Modeling and Control of a Low-Speed Flywheel Driving System for Pulsed-Load Mitigation in DC Distribution Networks," in *IEEE Transactions on Industry Applications*, vol. 52, no. 4, pp. 3378-3387, July-Aug. 2016.

[9] Mohamad El Hariri, Tarek A. Youssef, Abla Hariri and O. A. Mohammed, "Microgrids on Wheels: Not to Leave Security Behind," in IEEE Electrification Magazine (E-M), June 2016

[10] Mohamed, Ahmed Elsayed, Tarek. Youssef and O. A. Mohammed, "Wide-area monitoring and control for voltage assessment in smart grids with distributed generation," *Proceedings of the 2013 PES Innovative Smart Grid Technologies Conference (ISGT),* Washington, D.C., USA, 24-27 Feb 2013.

[11] Ahmed Elsayed, Tarek Youssef, A. Mohamed and O. A. Mohammed, "Design and Control of Standalone P-V System for Rural Residential Applications," *Fifth International Symposium on Energy ,Puerto Rico Energy Center-Laccei, February 7-8, 2013,Puerto Rico.*

[12] Tarek Youssef and O. A. Mohammed, " Adaptive SRF-PLL with Reconfigurable Controller for Microgrid in Grid-Connected and Stand-Alone Modes" *Proceedings of the 2013 Power and Energy Society General Meeting,* Vancouver, B.C., Canada, 21-25 Jul 2013.

[13] Tarek Youssef, A. Elsayed, A. Mohamed and O. A. Mohammed,"Intelligent Multi-Objective Control for Improved Integration of Microgrids to Power Systems Involving Highly Nonlinear Local Loads" ," *5th Innovative Smart Grid Technologies Conference (ISGT North America),* Washington, D.C., USA, 19-22 Feb 2014.