University of Strathclyde

Department of Electronic and Electrical Engineering

Facilitating the Validation of Adaptive Power System Protection through Formal Scheme Modelling and Performance Verification

Ibrahim Faiek Abdulhadi

A thesis presented in fulfilment of the requirements for the degree of Doctor of Philosophy

2013

This thesis is the result of the author's original research. It has been composed by the author and has not been previously submitted for examination which has led to the award of a degree.

Signed: *Ibrahim Abdulhadi* *Date:* *August 2013*

All praise to God for his endless guidance and sustenance

This thesis is dedicated to Imam Zaman (a.t.f.)

Acknowledgments

First and foremost I would like to express my thanks and gratitude to my supervisor Prof. Graeme Burt for his support and guidance during my studies. The challenges you continuously posed to my research definitely helped increase its quality. You always made me go the extra mile!

I would like to extend my thanks to my second supervisor Dr. Adam Dyśko. You always managed to provide an interesting and entertaining technical conversation.

Thanks to Dr. Ray Zhang of National Grid. I appreciate you facilitating my placement at the company and supporting my research work.

Thanks also go to the EPSRC for providing the financial support for this work and facilitating a UK forum for disseminating my research achievements.

I would also like to thank my colleagues in the department of electronic and electrical engineering whom with I had valuable research exchanges. Special thanks go to those who tolerated my cynicism on various topics of life.

Thanks to my brother for appreciating the comic value of my PhD experience and listening intently to related rants.

Finally and most importantly, sincere thanks go to my caring and loving parents for all their support, patience and prayers. Their continuous encouragement has proven invaluable especially during the writing of this thesis.

Abstract

There exists a critical mass in research related to adaptive protection approaches that address some of the shortcomings of conventional protection functions. This is in response to concerns in the reliability of conventional protection which manifested itself in some severe disturbances in more recent years. Despite the fact that adaptive protection offers a compelling technical solution to some of these performance problems, the industry has not widely adopted adaptive protection approaches as a de facto policy for future protection scheme implementations.

This is attributed to the difficulties associated with the testing of such schemes where no significant work has been reported yet. Furthermore, the benefits vs. the risks associated with such a protection strategy are not well understood. This is coupled with the conservatism towards radical changes in the way the power system is operated. As such the work reported in this thesis complements the existing body of research in order to address some of the major technical and institutional challenges associated with adopting adaptive protection schemes for future networks, especially those networks that exhibit flexibility in operation to deal with uncertainty in generation and to maximise asset utilisation. These are network characteristics that adaptive protection approaches are seen to be an effective enabler of.

This thesis focuses on formal structural and behavioural modelling of adaptive protection schemes as means to effectively validate their functional operation and verify their performance. Novel contributions have been made in formalising a user requirements driven architecture for these schemes. Furthermore, significant contributions have been made to conducting formal algorithm verification that complements inherently limited standard protection scheme validation techniques. The thesis makes thorough use of a proposed adaptive distance protection scheme for circuits with quadrature booster transformers to communicate the challenges, lessons learned and contributions in designing, implementing and testing adaptive protection schemes.

Contents

1 Introduction 25

1.1 Research context and justification 25

1.2 Research main hypothesis and contributions 27

1.3 Publications 28

1.4 Thesis outline 30

1.5 References 32

2 A Modern Perspective on Power System Protection 33

2.1 Chapter methodology and contributions 33

2.2 Power system protection principles 34

2.2.1 Unit-based protection 34

2.2.2 Non-unit based protection 36

2.3 Distance protection 37

2.3.1 Elements, characteristics and polarisation 37

2.3.2 Ground fault detection 41

2.3.3 Communications based distance schemes 42

2.3.4 Distance protection application issues and considerations 43

2.4 DER interface protection 45

2.4.1 Loss of mains protection 45

2.5 System integrity protection schemes 46

2.6 Wide area measurement, protection, automation and control 47

2.6.1 Synchrophasor measurement technology 47

2.6.2 Protection applications of SMT 48

2.7 The digital substation 49

2.7.1 Intelligent electronic devices 49

2.7.2 IEC 61850 communications standard 52
2.8 Functional testing of power system protection 54
2.8.1 Functional type testing 54
2.8.2 Software type testing 55
2.8.3 Commissioning testing 56
2.8.4 Shortfalls of existing testing practices 56
2.9 Chapter summary 57
2.10 References 57
3 Evaluating the Performance of Existing Protection Schemes under Flexible Primary System Operation 61
3.1 Chapter methodology and contributions 61
3.2 Causes of deterioration in protection performance under flexible power system operation 64
3.2.1 Flexible operation of the primary power system 64
3.2.2 Power system topology changes 65
3.2.3 Utilisation of DER 67
3.2.4 FACTS and similar devices providing system operational support 67
3.2.5 Wide-area disturbances 68
3.2.6 Hidden failures 68
3.2.7 Closing discussion on performance issues 69
3.3 Overview of quadrature booster transformers 70
3.3.1 QB construction, connection arrangements and functions 70
3.3.2 QB control and protection arrangements 72
3.3.3 Setting of distance protection for transmission lines with QBs 74
3.3.4 Coordinated control of QBs 74

3.4 The evaluation of the impact of QBs on distance protection performance 75
3.4.1 Evaluation methodology 75
3.4.2 QB model 76
3.4.3 Results of the distance protection reach evaluation 78
3.4.4 Discussion of reach impact due to QB operation 87
3.4.5 A relation for measured impedance error vs. QB mode 88
3.5 Sensitivity and stability evaluation of loss of mains protection 93
3.5.1 Methodology 94
3.5.2 Power system models 96
3.5.3 Compromise settings for DFIG based generation 97
3.5.4 Performance discrepancies between different ROCOF algorithms 97
3.6 Robust vs. flexible protection scheme performance 100
3.6.1 Robust behaviour of protection systems 100
3.6.2 The need for flexible power system protection 101
3.6.3 Robustness in protection measurement algorithms 103
3.7 Chapter summary 104
3.8 References 105
4 Delivering Flexible Protection Schemes with Enhanced Performance using an Adaptive Protection Philosophy 109
4.1 Chapter methodology and contributions 109
4.2 Adaptive protection concept review 111
4.2.1 Identification of prevailing power system conditions 111
4.2.2 Adaptable protection functions 113
4.2.3 Automatic adjustments of protection functions 115
4.3 Review of techniques to achieve adaptive protection functionality 116

4.3.1 Adaptive protection to improve scheme sensitivity 117
4.3.2 Adaptive protection to improve scheme coordination 119
4.3.3 Shaping the research direction for adaptive protection 120
4.4 Challenges to adopting adaptive protection 121
4.4.1 Integration with existing protection arrangements 121
4.4.2 Adaptive scheme testing 122
4.4.3 Inadequacy of utility policies and procedures 122
4.5 Using settings groups to enhance distance protection performance in QB presence 124
4.5.1 General strategy for the adaptive distance protection scheme 124
4.5.2 Settings group calculation and mapping to power system states 126
4.5.3 Settings group for a fall back situation 131
4.5.4 Settings group selection implementation with a physical relay ... 132
4.6 Choosing the number of settings groups for adaptive protection 134
4.7 Chapter summary 136
4.8 References 137
5 Requirements specification, architectural design and overall validation of adaptive protection schemes 140
5.1 Chapter methodology and contributions 140
5.2 Overview of adaptive protection design and architectures 141
5.3 Adaptive protection lifecycle requirements 143
5.3.1 Scheme design and implementation requirements 145
5.3.2 Scheme installation and commissioning requirements 146
5.3.3 Scheme operation and maintenance requirements 147
5.3.4 Scheme decommissioning and replacement requirements 148
5.3.5 Validation vs. verification of adaptive protection schemes 148

5.4 Development of a detailed adaptive protection architecture 150
5.4.1 The role of execution layer functions 150
5.4.2 The role of coordination layer functions 153
5.4.3 The role of management layer functions 154
5.5 Design and implementation of the proposed adaptive distance protection scheme 156
5.5.1 Primary 'system state acquisition' function 159
5.5.2 'Online protection performance verification' function 160
5.5.3 'New protection configuration selection' function 161
5.5.4 'New protection configuration activation and verification' function 162
5.5.5 Implemented communications interfaces 162
5.5.6 Management layer functions implementation 163
5.6 Hardware in the loop (HIL) adaptive distance protection scheme validation 164
5.6.1 HIL validation methodology 164
5.6.2 HIL validation results 165
5.6.3 Discussion of HIL validation results in light of APA design and scheme implementation 172
5.7 The role of hardware in the loop approach to validating adaptive protection schemes 174
5.8 Chapter summary 175
5.9 References 176
6 Formal approach to the verification of adaptive protection scheme performance based on hybrid systems modelling 178
6.1 Chapter methodology and contributions 178
6.2 Power system modelling in the hybrid system domain 180

6.2.1 Hybrid dynamical systems overview....180
6.2.2 Modelling power systems in the hybrid domain....181
6.3 Verification of hybrid systems performance....183
6.3.1 The use of reachability analysis to verify hybrid system safety ...184
6.3.2 Justification for conducting reachability analysis for adaptive protection safety verification....185
6.4 Defining a hybrid model for the developed adaptive distance protection scheme....186
6.4.1 Developing a DES abstraction to include adaptive protection functionality....186
6.4.2 Definition of operation and performance states as a prerequisite for reachability analysis....194
6.5 Reachability analysis for the verification of the developed adaptive distance protection logic....195
6.5.1 Reachability verification implementation in Simulink....197
6.5.2 Reachability analysis test setup and results....201
6.6 Discussion of reachability results and the role of formal approaches to the verification of adaptive protection functionality....205
6.7 Chapter summary....206
6.8 References....207
7 Thesis Conclusions and Future Work....209
7.1 Qualitative reflection on the general hypothesis....209
7.2 Evaluation of conventional protection performance....209
7.3 Design of adaptive protection schemes....211
7.4 Structural and behavioural modelling of adaptive protection schemes....212
7.5 Validation and verification of adaptive protection schemes....213

7.6 Future work.....215

Appendix A Test transmission network model data and protection settings.....216

Appendix B Adaptive Distance Protection Simulink Model .218

Appendix C Load encroachment test scenario.....228

List of Figures

Figure 2-1 A typical current differential protection scheme showing zone of protection 35
Figure 2-2 Radial distribution network showing grading between IDMT characteristics to achieve selectivity between overcurrent protection relays ... 36
Figure 2-3 Mho distance protection characteristic 39
Figure 2-4 Quadrilateral characteristic showing independently adjustable resistive and reactive reaches 40
Figure 2-5 Distance protection zones 40
Figure 2-6 Zone 2 coordination with shortest adjacent line 41
Figure 2-7 Load blinders used to minimise load encroachment 43
Figure 2-8 Distance protection of multi-terminal circuits 44
Figure 2-9 Typical WAMPAC architecture 48
Figure 2-10 IED hardware architecture 49
Figure 2-11 Typical PSL diagram 51
Figure 2-12 IEC 61850 functional hierarchy 52
Figure 2-13 Typical substation architecture utilising IEC 61850 53
Figure 2-14 Dynamic type testing of protection relays 55
Figure 3-1 Schematic showing QB shunt and series elements 70
Figure 3-2 QB phasor diagram showing primary system quantities incorporating QB action 71
Figure 3-3 QB substation connection arrangement 72
Figure 3-4 Typical QB operating envelope 73
Figure 3-5 Typical QB local control system 73
Figure 3-6 Modelled primary system single line diagram showing QB positions 76
Figure 3-7 QB in extended delta winding connection 77
Figure 3-8 QB introduced phase shift vs. tap position 77
Figure 3-9 Circuit power flow vs. QB tap position 77
Figure 3-10 Fault impedance when QB is in Bypass mode 85
Figure 3-11 Fault impedance when QB is in Boost mode 86

Figure 3-12 Fault impedance when QB is in buck mode 87
Figure 3-13 Mho characteristic showing how the reach error magnitude is measured 90
Figure 3-14 Mho diagram illustrating process of determining $|Z_{offset}|$ 92
Figure 3-15 LOM sensitivity and stability testing procedure 95
Figure 3-16 33kV test network 96
Figure 3-17 11kV Test network 96
Figure 3-18 Maximum sensitivity settings for 30MVA synchronous DG connected to 33kV network – relay 1 98
Figure 3-19 Maximum sensitivity settings for 30MVA synchronous DG connected to 33kV network - relay 2 98
Figure 3-20 Maximum sensitivity settings for 30MVA synchronous DG connected to 33kV network - relay 3 99
Figure 3-21 Primary current trajectory under normal operating conditions 101
Figure 3-22 Flexible changes in protection setting and new system current trajectory 102
Figure 4-1 Adaptive protection scheme composition 115
Figure 4-2 Adaptive distance protection general strategy 126
Figure 4-3 Phase to phase fault impedance locus mapping on Mho diagram with different QB modes, tap positions and fault positions 127
Figure 4-4 Mho diagram showing extended zone 2 (AZ) for QB boost mode 128
Figure 4-5 Mho diagram showing extended zone 2 (AZ) for QB buck mode to fully offset under reach issue 129
Figure 4-6 Mho diagram showing extended zone 2 (AZ) for QB buck mode to partially offset under reach issue 129
Figure 4-7 Mho diagram showing extended zone 3 (AZ) for QB buck mode 130
Figure 4-8 Settings group selection implementation 132
Figure 4-9 Alstom P446 PSL for settings group selection 133
Figure 4-10 Using IEC 61850 for selecting between a large number of settings groups 134
Figure 5-1 Original proposed adaptive protection architecture 141
Figure 5-2 Development of requirements for a system 144

Figure 5-3 Behaviour of adaptive scheme under SCT and normal operating modes 146
Figure 5-4 V-Model for the V&V of a system's design and implementation 149
Figure 5-5 Developed adaptive protection architecture 151
Figure 5-6 High level structure of the Simulink model and interaction with testing 157
Figure 5-7 Adaptive distance protection scheme implementation 158
Figure 5-8 Physical equipment used for HIL testing of the adaptive distance protection scheme 159
Figure 5-9 QB connection and mode state acquisition 160
Figure 5-10 Initiating or blocking settings changes based on reach error for a given QB state 161
Figure 5-11 Settings activation low level implementation 162
Figure 5-12 Test network showing fault positions and distance protection relay 165
Figure 5-13 Test case 1, adaptive protection disabled 166
Figure 5-14 Test case 1, adaptive protection enabled 166
Figure 5-15 Test case 1, IED disturbance record 166
Figure 5-16 Test case 2, adaptive protection disabled 167
Figure 5-17 Test case 2, adaptive protection enabled 167
Figure 5-18 Test case 2, IED disturbance record 168
Figure 5-19 Test case 3, adaptive protection disabled 168
Figure 5-20 Test case 3, adaptive protection enabled 169
Figure 5-21 Test case 3, IED disturbance record 169
Figure 5-22 Test case 4, adaptive protection disabled 170
Figure 5-23 Test case 4, adaptive protection enabled 170
Figure 5-24 Test case 4, IED disturbance record 170
Figure 5-25 Test case 5, adaptive protection disabled 171
Figure 5-26 Test case 5, adaptive protection enabled 171
Figure 5-27 Test case 5, IED disturbance record 172
Figure 6-1 Basic DES abstraction of a hybrid system 181
Figure 6-2 System under consideration for behavioural modelling 186

Figure 6-3 Finite state machine representing operating states of protection element 187
Figure 6-4 Interactions between continuous and discrete components of system under study 191
Figure 6-5 DES abstraction representing adaptive protection functionality and its relation to conventional protection elements and the underlying primary system 192
Figure 6-6 Finite automata reflecting primary plant states 193
Figure 6-7 Partitioning of the hybrid state space 194
Figure 6-8 Reachability analysis procedure 197
Figure 6-9 Reachability analysis subsystem 198
Figure 6-10 Stateflow subsystem for reachability analysis showing three categories under test 199
Figure 6-11 Reach performance Stateflow state diagram (automaton) 200
Figure 6-12 Load encroachment performance Stateflow state diagram 200
Figure 6-13 Adjacent line coordination performance Stateflow diagram 201
Figure 6-14 Structure of the Simulink test harness for performing reachability analysis 202
Figure 6-15 QB states for stimulating the adaptive protection logic using a PRBS 202
Figure 6-16 Correct operation of adaptive logic indicated by safe states 203
Figure 6-17 Failure of adaptive logic leading to unsafe state detection 204
Figure B-1 Full high level Simulink model showing constituent subsystems 218
Figure B-2 Signal generator for testing the model 219
Figure B-3 Coordination layer subsystems 220
Figure B-4 Primary system state acquisition subsystems 221
Figure B-5 Stateflow chart to determine QB state based on status measurements 221
Figure B-6 Stateflow chart used to determine line loading state based on status measurements 222
Figure B-7 Protection performance verification subsystem 223
Figure B-8 Protection settings selection subsystem 224

Figure B-9 Setting activation and verification subsystem 225
Figure B-10 Reachability analysis signal mapping subsystem 226
Figure B-11 Staeflow chart mapping QB state and protection setting for reachability analysis 227
Figure B-12 Management layer functionality 227
Figure B-13 Reachability analysis subsystem 227
Figure C-1 Transmission circuit used for load encroachment 228
Figure C-2 Mho characteristic showing impedance pre and post load encroachment 229

List of Tables

Table 2-1 Typical distance protection zone settings 41
Table 2-2 Common communications based distance schemes and their application 42
Table 3-1 Measured impedance and impedance error for faults at 0% line length 79
Table 3-2 Measured impedance and impedance error for faults at 30% line length 80
Table 3-3 Measured impedance and impedance error for faults at 50% line length 81
Table 3-4 Measured impedance and impedance error for faults at 70% line length 82
Table 3-5 Measured impedance and impedance error for faults at 100% line length 83
Table 3-6 Measured impedance for resistive faults at 50% line length 84
Table 3-7 Measured impedance for phase to phase fault at 50% line length for simultaneous QB operation 84
Table 3-8 Variables used for the estimation of impedance error magnitude 92
Table 3-9 Compromise relay 1 ROCOF settings for 3MVA DFIG generator connected to 11kV network 97
Table 4-1 Settings groups selected for the adaptive distance protection scheme 130
Table 4-2 Active settings groups using the relay binary inputs 132
Table 4-3 Recommended number of settings groups indicating reach improvement 136
Table 5-1 Implemented settings groups 162
Table 5-2 Summary of hardware in the loop test cases for the adaptive protection scheme 164
Table 1 Summary of continuous and discrete dynamics in the hybrid system model 190
Table 2 Safety conditions for adaptive logic under test 202

Table A-1 Substation data for test transmission network.....216
Table A-2 Distance relay model configuration and related data.....216
Table A-3 Distance relay model zone reach and delay settings 217
Table A-4 National Grid network section data used for distance reach studies 217
Table C-1 Transmission network model data 228

List of abbreviations

AEZ	Anti-Encroachment Zone
ANN	Artificial Neural Network
APA	Adaptive Protection Architecture
COMTRADE	Common format for Transient Data Exchange
CT	Current Transformer
CVT	Capacitive Voltage Transformer
DAR	Delayed Auto Reclose
DER	Distributed Energy Resources
DES	Discrete Event System
DFIG	Doubly Fed Induction Generator
DG	Distributed Generation
DMS	Distribution Management System
DNP3.0	Distributed Network Protocol 3.0
DO	Data Object
DT	Definite Time
DUT	Device Under Test
EMC	Electro Magnetic Compatibility
EMS	Energy Management System
FACTS	Flexible AC Transmission Systems
FCL	Fault Current Limiter
GA	Genetic Algorithm

GOOSE	Generic Object Oriented Substation Event
GPS	Global Positioning System
HDS	Hybrid Dynamical System
HIL	Hardware in the Loop
HMI	Human Machine Interface
ICT	Information and Communications Technology
IDMT	Inverse Definite Minimum Time characteristic
IED	Intelligent Electronic Device
LAN	Local Area Network
LED	Light Emitting Diode
LN	Logical Node
LOM	Loss of Mains
MAS	Multi Agent System
MTTR	Mean Time to Repair
MU	Merging Unit
NCIT	Non-Conventional Instrument Transformer
OLTC	On Load Tap Changer
OPC	Object Linking and Embedding for Process Control
PC	Personal Computer
PCC	Point of Common Coupling
PD	Physical Device
PMU	Phasor Measurement Unit

PRBS	Pseudo Random Binary Sequence
PSL	Programmable Scheme Logic
PSO	Particle Swarm Optimisation
PST	Phase Shifting Transformer
QB	Quadrature Booster
QBCS	Quadrature Booster Control System
RCA	Relay Characteristic Angle
ROCOF	Rate of Change of Frequency
RTDS	Real Time Digital Simulator
SCL	Substation Configuration Language
SCT	Site Commissioning Test
SG	Setting Group
SGCB	Settings Group Control Block
SIPS	System Integrity Protection System
SMT	Synchrophasor Measurement Technology
SV	Sampled Value
V&V	Verification and Validation
VS	Voltage Vector Shift
VT	Voltage Transformer
WAMPAC	Wide Area Measurement, Protection and Control
WAMS	Wide Area Measurement System
XML	Extensible Mark-up Language

List of symbols

k_0	Ground fault zero sequence compensation factor
k_n	Ground fault residual compensation factor
$\|\Delta Z\|$	Reach error magnitude (Ω)
δ	Reach error threshold (Ω)
I_0	Zero sequence current (A)
I_n	Residual current (A)
Z_0	Zero sequence impedance (Ω)
Z_1	Positive sequence impedance (Ω)
R_0	Zero sequence resistance (Ω)
R_1	Positive sequence resistance (Ω)
X_0	Zero sequence reactance (Ω)
X_1	Positive sequence reactance (Ω)
B_0	Zero sequence susceptance (S)
B_1	Positive sequence susceptance (S)
Z_s	Positive sequence source impedance (Ω)
H	Hybrid system automaton
Q	Set of discrete states
Q_{pps}	Primary power system operational state
Q_{cps}	Conventional protection system operational state
X	Set of continuous states

In	Set of hybrid system inputs
$Init$	Set of initial hybrid system states
Dom	Discrete state domain
E	Set of edges/transition maps
f	Continuous vector field
G	Set of guard conditions
R	Continuous state reset relation
q_n	Discrete state n
$\mathbb{R}$	Set of real numbers
S_n	Active setting n
T_n	State transition n
$\bar{G}$	Unsafe state space
ξ_p	Invariant performance state
I_{enc}	Load encroachment threshold current
$x(t)$	Monitored system quantities
$\tilde{x}[n]$	Event related to monitored system quantities
$\tilde{r}[n]$	Protection event
$r(t)$	Protection command
◊	Eventually logical operator
□	Always logical operator
|	AND logical operator

1 Introduction

1.1 Research context and justification

Approaches to power system protection are under scrutiny for mal-operation and shortcomings in performance which leave the power system exposed during dynamic and stressed system operating conditions. The dynamic system operation and the uncertainties brought with it were some the main focuses of the research consortium SUPERGEN FlexNet that funded the research reported in this thesis. These operational challenges have been echoed by the protection research community that identified a number of issues that affect the performance of protection schemes. Such issues include:

- Topological changes in the power system and transmission and distribution levels result in changes in fault levels that affect the operating times or even the sensitivity of protection or changes fault paths that affect the coordination of protection [1, 2].
- The impact of power electronic generator and energy storage interfaces on the fault levels seen by protection which can affect their sensitivity especially in islanded power system operation [3, 4].
- Operating the power system with lower inertia due to the connection of large levels of wind generation, in addition to the increased utilisation of the transmission network can result in more forceful system disturbances. This can affect the performance of system protection especially those relying on system frequency to operate [5, 6].

One of the approaches to improve the protection functionality, as proposed in the literature, relies on adaptive techniques. These involve dynamic changes in the protection functionality to reflect the state of the power system at any given time. These dynamic changes in protection configuration are governed by specially designed and often bespoke logic. This logic can rely on simple mappings between system states and new protection configurations or more complex arrangements that utilise intelligent systems or optimisation techniques [7, 8]. System operators are also expressing interest in adaptive protection. Smart grid projects funded by the low carbon network fund (LCNF) scheme consider adaptive protection in their demonstration [9]. But the more pressing issue is that the philosophy of adaptive protection was never fully embraced by the power system operators despite the clear performance enhancements that they provide and the clear need to achieve such improvement in performance.

There are some fundamental problems related to adaptive protection that are not being addressed sufficiently or are being outright ignored. For instance, issues related to testing the adaptive schemes out with a set of very specific case studies are rarely discussed. No standard or widely accepted approaches to testing exist. Furthermore, the requirements development for adaptive protection schemes is fairly basic despite it being an important prerequisite for scheme validation and verification. Furthermore, it is important to consider the implications of gradually introducing more adaptive protection schemes alongside more conventional approaches to protection. As such, there must be strategies for non-intrusive integration of these protection schemes to substations as well appropriate revisions for related utility policies.

To this end, the work reported in this thesis complements the body of research related to adaptive power system protection. This is achieved by identifying the barriers to the adoption of such techniques and approaches to facilitate their adoption where needed. In doing so, this thesis answers three pertinent research questions:

- How much flexibility can adaptive protection provide and where can it be applied without adding an unmanageable level of uncertainty to the power system operation?
- How can adaptive protection functions be integrated in a substation without the need for an overhaul in protection scheme design or equipment?
- How should the testing methodology for adaptive protection be approached in order to de-risk the behaviour of such schemes?

1.2 Research main hypothesis and contributions

The following statements describe the main research hypothesis:

Power systems that are operated in a flexible manner necessarily require protection schemes that display flexible operating characteristics. Adaptive protection techniques strategically integrated within substations can deliver the required level of flexible operation without jeopardising required performance levels.

From these statements, a number of sub-hypotheses are examined throughout the course of this thesis:

- Existing protection scheme testing practices are not sufficiently effective in validating the overall adaptive scheme functionality and existing practices must be complemented but not completely revamped.
- In order to de-risk the adaptive protection functionality, a description of its behaviour is required such that it takes into account the state of the power system, the configuration of the protection scheme and dynamic interactions between both systems.
- Achieving the flexibility required from adaptive protection can be achieved effectively through functional integration with existing relaying platforms and conventional protection elements.

The development of a lab based adaptive protection using commercial distance protection functions and substation automation equipment served as a vehicle to test the hypotheses made earlier. To this end, four main novel contributions have been made. These are:

- An experimentally validated adaptive distance protection scheme has been developed. It is based on dynamic settings group selection to improve the performance of distance protection in the presence of quadrature booster transformers (QB). This provides an improvement in reach of up to 20% for distance zones that are affected by the under-reach effect of the QB.
- The adaptive protection architecture proposed in previous work, which is adopted by the developed adaptive distance protection scheme, was formalised and validated using a system's engineering approach. This considered the functional requirements of an adaptive protection scheme over its lifecycle and utilised model based design using Simulink to create platform independent adaptive protection functions.
- Limitations in the standard method of hybrid modelling abstraction (which is used in this thesis to model the behaviour of the adaptive protection) were overcome. This was achieved by extending the behavioural model to accommodate concurrent control loops which encompasses the adaptive protection functionality.
- A powerful approach to formally verify the logic of adaptive protection schemes has been demonstrated. This method is based on a novel application of reachability analysis (safety property verification) to adaptive protection that utilises the developed hybrid behavioural model.

1.3 Publications

Journal articles:

- I. Abdulhadi, A. Dysko, G. Burt, "Reachability Analysis for the Verification of Adaptive Protection Setting Selection Logic," submitted to IEEE transactions on Power Delivery.

- A. Roscoe, I. Abdulhadi, G. Burt, "P and M Class Phasor Measurements Unit Algorithms using Adaptive Cascaded Filters," IEEE transactions on Power Delivery, 2013.

Conference papers:

- I. Abdulhadi, R. M. Tumilty, G. M. Burt, and J. R. McDonald, "A dynamic modelling environment for the evaluation of wide area protection systems," in *Universities Power Engineering Conference, 2008. UPEC 2008. 43rd International*, 2008, pp. 1–5.
- I. Abdulhadi, G. M. Burt, A. Dysko, R. Zhang, and J. Fitch, "The evaluation of distance protection performance in the presence of Quadrature Boosters in support of a coordinated control strategy," in *Developments in Power System Protection (DPSP 2010). Managing the Change, 10th IET International Conference on*, 2010, pp. 1–5.
- I. Abdulhadi, F. Coffele, A. Dysko, C. Booth, and G. Burt, "Adaptive Protection Architecture for the Smart Grid," in *Innovative Smart Grid Technologies (ISGT 2011).* 2011, pp. 1–8.
- S. P. Le Blond, R. K. Aggarwal, I. F. Abdulhadi, and G. M. Burt, "Impact of DFIG windfarms and instrument transformers on transient based protection," in *Developments in Power System Protection (DPSP 2010). Managing the Change, 10th IET International Conference on*, 2010, pp. 1–5.
- J. Kincaid, I. Abdulhadi, A. Emhemed, G. Burt, "Evaluating the Impact of Superconducting Fault Current Limiter on the Performance of Distribution Network Protection Schemes," in *Universities Power Engineering Conference, 2011. UPEC 2011. 46th International*, 2011, pp. 1-6.
- V. Terzija, P. Regulski, L. P. Kujunmuhammed, B. C. Pal, G. Burt, I. Abdulhadi, T. Babnik, M. Osborne, W. Hung, "FlexNet Wide Area Monitoring System," in *IEEE PES General Meeting*, 2011, pp. 1-7.
- Roscoe, I. Abdulhadi, G. Burt, "P-Class Phasor Measurement Unit Algorithms Using Adaptive Filtering to Enhance Accuracy at Off-Nominal Frequencies," in *Smart Measurements for Future Grids, IEEE International Conference on*, 2011, pp. 1-8.

- X. Cao, I. Abdulhadi, C. Booth, G. Burt, "Defining the Role of Wide Area Adaptive Protection in Future Networks", in *Universities Power Engineering Conference, 2011. UPEC 2011. 47th International*, 2012, pp. 1-6.
- I. Abdulhadi, F. Coffele, A. Dysko, C. Booth, G. Burt, G, Lloyd, B. Kirby, "Performance Verification and Scheme Validation of Adaptive Protection Schemes", in *CIGRE 2012 Session*, 2012, pp. 1-9.
- A. Adrianti, I. Abdulhadi, A. Dysko, G. Burt, "Assessing the reliability of adaptive power system protection schemes", in *Developments in Power System Protection (DPSP 2012). 11th IET International Conference on*, 2012, pp. 1-6.
- L. Xiong, I. Abdulhadi, G. Burt, "Adaptive Load Blinder for Maximising Distance Protection Loadability," PACWorld 2013.

National and international reports:

- DERlab, "International White Book on DER Protection: Review and Testing Procedures", 2011.
- Energy Network Association, "ETR 139:2009, Recommendations for the Setting of Loss of Mains Protection Relays", 2009.

1.4 Thesis outline

The remainder of the thesis chapters are laid out as follows:

Chapter 2 – a review of power system protection fundamentals is presented in this chapter. This chapter focuses on distance protection and loss of mains protection as these protection concepts are revisited over the course of the thesis. The chapter also presents recent advances and emerging approaches to protection including wide area protection systems based on synchrophasor measurement technology and the application of the IEC 61850 international standard to substation automation. The chapter also discusses different methods for the testing of protection schemes and highlights some of the challenges associated with the testing of new approaches to protection.

Chapter 3 – claims of conventional protection performance shortfalls have been substantiated in this chapter through a combination of literature review, simulations and laboratory testing. The chapter focuses on protection performance issues that stem from the varied and flexible operation of future power systems. Simulations conducted have quantified the effect quadrature booster transformers have on the reach of distance protection. Furthermore, the performance of loss of mains protection (mainly ROCOF) was evaluated using secondary injection testing. The chapter finally asserts that to overcome protection performance challenges caused by flexible power system operation a flexible approach to protection is required.

Chapter 4 – this chapter reviews adaptive protection methods as an approach to provide the required flexibility for protection scheme functionality and thus enhance its performance. This review focuses on adaptive protection techniques that improve the selectivity or coordination of protection schemes. By recognising the technical and institutional challenges facing the adoption of an adaptive protection strategy, the chapter identifies the scope adaptive protection functionality where it is considered most applicable. The chapter finally provides a preliminary design for an adaptive distance protection scheme based on multiple settings groups to address problems identified in the previous chapter.

Chapter 5 – a systems engineering based approach to adaptive protection is presented here. It focuses on developing life-cycle functional requirements for adaptive protection schemes which are reflected in a formalised adaptive protection architecture. An architecture compliant design and implementation of the adaptive distance protection scheme is presented. Hardware in the loop testing is used to validate the scheme in full view of the developed requirements and architecture.

Chapter 6 – this chapter develops a behavioural representation of adaptive protection functionality using hybrid systems modelling which combines discrete and continuous system dynamics in a finite automaton. It focuses on

using this behavioural representation to extract a measure of adaptive protection performance (adaptive protection safety) and verify it using reachability analysis. The adaptive setting logic used by the distance protection scheme developed in the thesis was verified using reachability analysis.

Chapter 7 – the main thesis conclusions are presented in this chapter with a focus on contributions made to the power system protection community and the systems verification body of research. Future directions of research have also been identified with focus on applying the modelling and testing methodologies developed in this thesis to wide area protection schemes.

1.5 References

[1] F. Coffele, C. Booth, G. Burt, C. McTaggart, and T. Spearing, "Detailed Analysis of the Impact of Distributed Generation and Active Network Management on Network Protection Systems," in *CIRED 2011*, 2011.

[2] D. Tholomier and A. Apostolov, "Adaptive protection of transmission lines during wide area disturbances," in *Power Systems Conference and Exposition, 2009. PSCE '09. IEEE/PES*, 2009, pp. 1-7.

[3] E. Sortomme, G. J. Mapes, B. A. Foster, and S. S. Venkata, "Fault analysis and protection of a microgrid," in *Power Symposium, 2008. NAPS '08. 40th North American*, 2008, pp. 1-6.

[4] M. A. Zamani, T. S. Sidhu, and A. Yazdani, "A Protection Strategy and Microprocessor-Based Relay for Low-Voltage Microgrids," *IEEE Transactions on Power Delivery,* vol. 26, pp. 1873-1883, 2011.

[5] NGET, "Report of the national grid investigation into the frequency deviation and automatic demand disconnection that occured on the 27th May 2008," 2009.

[6] R. Doherty, A. Mullane, G. Nolan, D. J. Burke, A. Bryson, and M. O'Malley, "An Assessment of the Impact of Wind Generation on System Frequency Control," *IEEE Transactions on Power Systems,* vol. 25, pp. 452-460, 2010.

[7] M. Sanaye-Pasand and P. Jafarian, "An Adaptive Decision Logic to Enhance Distance Protection of Transmission Lines," *IEEE Transactions on Power Delivery,* vol. 26, pp. 2134-2144, 2011.

[8] M. M. Mansour, S. F. Mekhamer, and N. E. S. El-Kharbawe, "A Modified Particle Swarm Optimizer for the Coordination of Directional Overcurrent Relays," *IEEE Transactions on Power Delivery,* vol. 22, pp. 1400-1410, 2007.

[9] UKPN, "Flexible plug and play for low carbon networks - LCNF funding submission," 2011.

2 A Modern Perspective on Power System Protection

2.1 Chapter methodology and contributions

Modern substation technologies provide the building blocks for the realisation of new and improved protection techniques and systems. This chapter examines the fundamental concepts and recent developments in power system protection practices. A brief explanation of distance protection principles is included as it will be revisited in later chapters of the thesis. Other functions will not be discussed in detail as they have been treated exhaustively in previous theses and related textbooks. Focus will also be placed on the emerging concepts of the digital substation and wide area protection systems. Finally, the testing of protection schemes will be discussed while identifying potential shortfalls of existing testing practices. This will be used as a springboard for the development of improved functional testing methodologies in later chapters. All protection functions discussed in this chapter are based on numerical methods.

The main contributions of this chapter are:

- Review of emerging approaches to power system protection including those utilising synchrophasor technologies and digital substation functions.
- Discussion of limitations in protection system testing practices in coping with scheme developments and new functional requirements.

2.2 Power system protection principles

Although protection systems represent a 5% capital investment of the overall power system [1], they are considered a fundamental operational component. Without protection schemes, power systems cannot be operated in a stable, secure or reliable manner. Different protection functions are deployed in transmission and distribution networks. This is mainly due to the more stringent stability requirements placed on transmission networks [2]. Consequently more complex scheme configurations are found on transmission networks in addition to redundant schemes. Distribution networks on the other hand require more cost effective protection solutions due to the sheer volume of feeders and network assets that need to be protected [3].

Recent developments in distribution network automation in addition to the increased penetration of DG are stimulating more interest in distribution network protection [4]. This particular field has seen growth in research activity which led to the development of many improved protection functions including those dealing with protection performance issues arising from islanded network operation [5], changes in network topology [6], increased use of power electronics in generator interfaces [7], etc.

2.2.1 Unit-based protection

Zones of protection are used to define the areas of the primary system which are protected by a specific protection function. In a unit-based protection scheme (current differential for example), the zone of protection boundary is defined by the instrument transformers used to measure the current flow through the protected feeder as shown in Figure 2-1. Such schemes are mostly applied to transmission networks where the cost of required communications is justified. These schemes are also highly selective in their operation. However, they may suffer from instabilities if current transformers are saturated due to high through fault currents [8]. This can be mitigated by the use of new sensing technologies such as Rogowski coils, hall effect sensors or optical current sensors. These are referred to as non-conventional instrument transformers (NCITs) [8]. More recent developments make use of optical fibre Bragg gratings

to directly measure the line quantities without intermediate electrical/optical transformations. This allows for faster acquisition of line current from different points on the line using the same optical fibre [9].

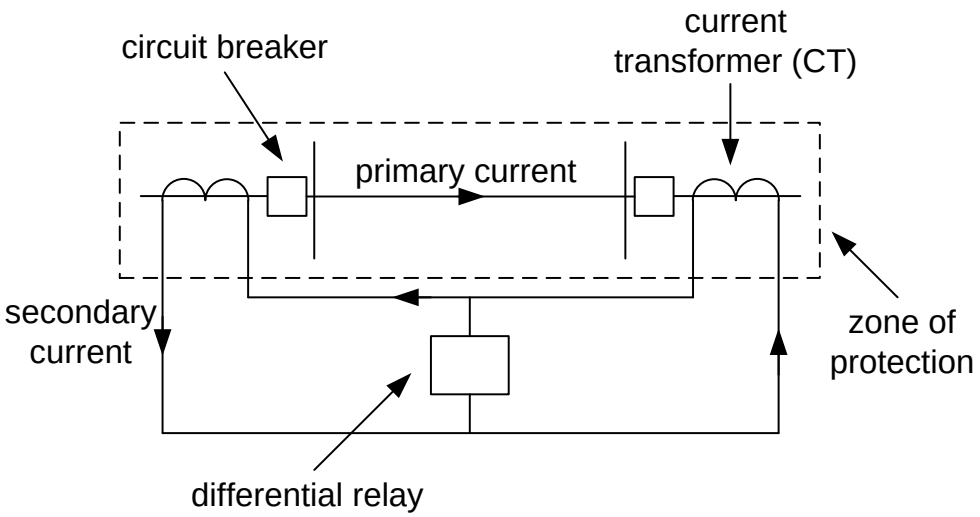

Figure 2-1 A typical current differential protection scheme showing zone of protection

Digital current differential protection relies on communications to exchange measurements made across the protection zone boundary. Dedicated point to point communications links are commonly used for this purpose. Such links' latencies can be characterised so that corresponding measurements made at different physical points can be compared at the same time regardless of communications channel delay. Alternatively, the delay compensation algorithms (e.g. ping pong method) can be used to dynamically calculate this delay and compensate for it [10]. With the advent of non-deterministic packet switched communications networks, compensating for channel delays becomes more problematic. To tackle this problem, GPS synchronisation can be used were each measurement can be tagged with a GPS time stamp [11]. Therefore, only corresponding measurements are compared. When backhaul communications infrastructure is used for exchanging measurements, routing technologies such as IP/MPLS (Internet Protocol/Multi-Protocol Label Switching) can guarantee the communications quality of service by prioritising protection traffic [12].

2.2.2 Non-unit based protection

Non-unit protection schemes can be found in both transmission and distribution networks. These rely on local measurements made by instrument transformers to inform the protection functions. Such functions include overcurrent and distance protection. The latter will be discussed in detail in the following section due to its relevance to the remainder of the thesis.

Overcurrent protection is mostly applied in distribution networks due to its simplicity. It is however also used in transmission networks as a backup protection function. Phase or earth faults are detected by simply measuring the current at the relaying point and comparing that with a predetermined pick-up setting. To achieve selectivity in operation, time delays or fault levels or a combination of both are used. The latter method is most commonly used and is achieved using an inverse definite minimum time (IDMT) characteristic as shown in Figure 2-2. The IDMT characteristic ensures that faster operation is achieved with higher fault currents. A time setting multiplier is used to coordinate the operation of relays in series (R1-R3) which creates a grading margin. The grading margin is selected based on breaker operating times, errors in the protection system and the overall acceptable operating time for the specific network.

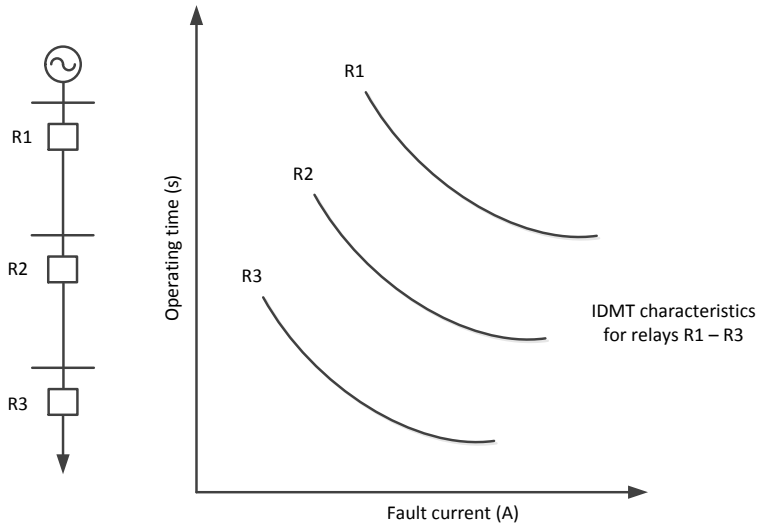

Figure 2-2 Radial distribution network showing grading between IDMT characteristics to achieve selectivity between overcurrent protection relays

One of the main issues facing the application of overcurrent protection is the increased penetration of distributed energy resources (DER) as well as changes in operation practices such as islanded network operation or the dynamic changes in network topology. These network operating conditions and their impact on protection performance will be examined further in chapter 3.

Overcurrent protection reach depends on fault type and source impedance [8, 13]. Thus its application as a main protection function to transmission lines is undesirable since non-selective operation can have a detrimental impact on system stability. Therefore, a protection method that is mostly independent of variable fault currents is necessary. Distance protection is an example of such a protection method.

2.3 Distance protection

Distance protection is mainly used in transmission systems. It is applied, to a lesser extent, in meshed distribution systems to improve selectivity with a faster operating time [14]. Distance protection relies on the simple principle that the protected line impedance is proportional to its length. Therefore, by measuring (or more practically calculating) the protected line impedance, a fault can be identified by monitoring changes in the impedance. These changes can then be compared with impedance characteristics to determine the need to operate or restrain [14]. Multiple distance relays can be made part of a communications based scheme. Such schemes are used to overcome reach issues or accelerate tripping of time delayed distance relays.

2.3.1 Elements, characteristics and polarisation

Distance protection relies on both current and voltage measurements in order to obtain the apparent impedance of the circuit at the relaying point. This is then compared with the relay settings which represent the distance protection reach (or protection zone boundary). A distance protection algorithm consists of six of these impedance calculation elements which correspond to each fault type in a three phase system – that is AG, BG, CG, AB, BC and CA short circuit

faults for an ABC three phase system where G represents ground. The apparent impedance is calculated as in (1, 2) [15]:

Earth fault:

$$Z_{ph-g} = V_{ph}/(I_L + k_0 I_0) \quad (1)$$

Phase fault:

$$Z_{ph1-ph2} = (V_{ph1} - V_{ph2})/(I_{L1} - I_{L2}) \quad (2)$$

Where Z_{ph-g} is the apparent impedance calculated by the relay for a phase to ground fault, $Z_{ph1-ph2}$ is the apparent impedance in a phase to phase fault situation, V_{ph} is the phase voltage, I_L is the line current, I_0 is the zero sequence current and k_0 is the a compensation factor used to compensate for the zero sequence current present during an earth fault [16]. More details on this factor will be given in the following section. Close up faults resulting in a large depression in measured voltage, below the minimum voltage level required for a reliable measurement, can result in incorrect identification of the faulty phases. This is problematic in single pole tripping schemes. To overcome this, phase selection logic is used. One method of realising phase selection is based on comparing pre and post fault quantities to determine the amount of step change to accurately identify the faulted phases [8].

Several operating characteristics exist for distance protection. Modern numerical relays provide the ability to create a custom characteristic. However, the most common ones used are the Mho and quadrilateral characteristics. The MHO characteristic, as shown in Figure 2-3, is self-polarised. The voltage measurement is used to restrict fault detection to those faults that occur downstream of the relay.

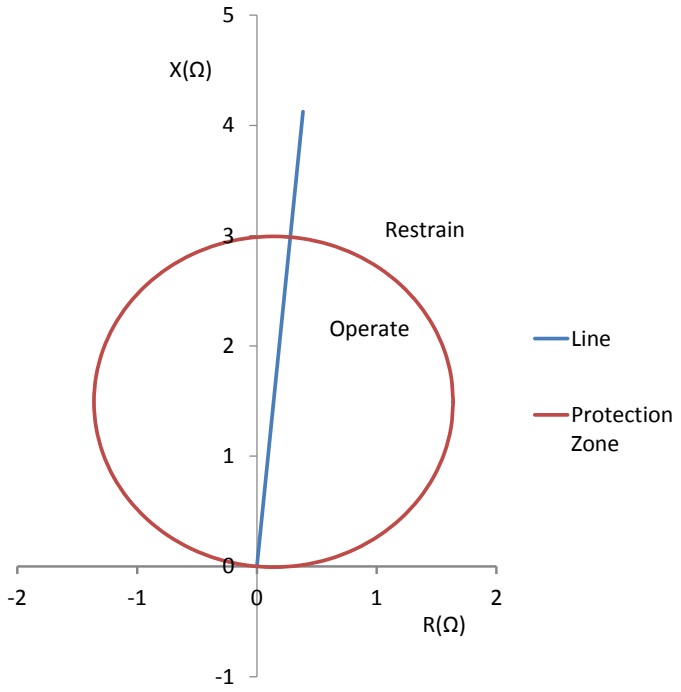

Figure 2-3 Mho distance protection characteristic

The area inside the characteristic is the operate region. The protected transmission line is inclined at its angle (e.g. 85° for a 400kV system with a 12 X/R ratio). Polarisation using healthy phase voltages is not possible during a three phase fault. Therefore, memory polarisation is used to overcome this. In this case, recent measurements of the faulty phase that are stored in the relay memory prior to fault inception are used. For non-symmetrical faults, healthy phases not affected by the fault can be used for polarisation which is known as cross polarisation [8].

Quadrilateral characteristics are mainly used to address the under-reach problem caused by resistive earth faults or arcing faults [17]. The resistive reach of the characteristic can be adjusted independently of the reactive reach as shown in Figure 2-4.

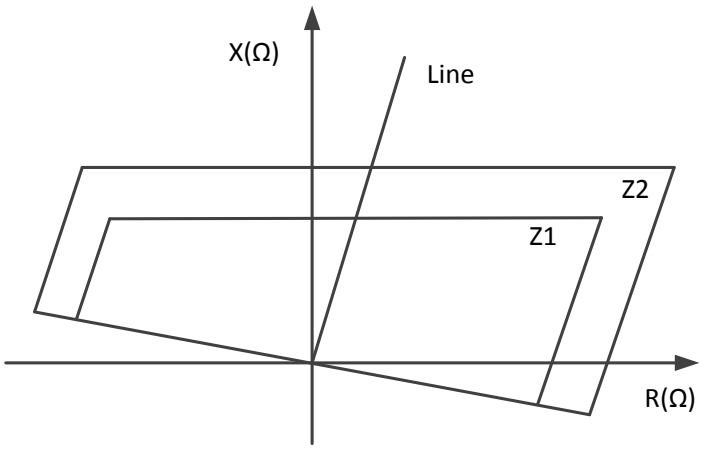

Figure 2-4 Quadrilateral characteristic showing independently adjustable resistive and reactive reaches

Plain (non-communications based) distance protection schemes are usually arranged in a stepped zone configuration (see Figure 2-5) to achieve remote backup functionality and, at the same time, coordinate with other distance schemes upstream of the relay. Each relaying point will usually have three active distance protection zones – zone 1, zone 2 and zone 3 (Z1–Z3). Each zone protects a predetermined circuit length and an appropriate time delay (e.g. t1 and t2) to coordinate between the different zones. Typical zone settings are summarised in Table 2-1 [8]. Zone 3 can be offset by 20% of the protected line length in order to provide backup protection for the local busbar.

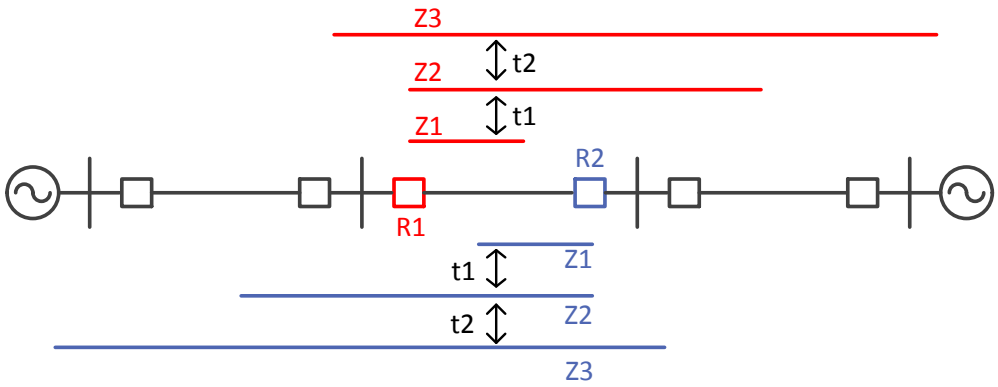

Figure 2-5 Distance protection zones

Table 2-1 Typical distance protection zone settings [8]

Distance Zone	Settings
Zone 1	80% of line impedance, instantaneous
Zone 2	100% of line impedance + 50% of shortest adjacent line, 0.5s delay
Zone 3	120% of line impedance and longest adjacent line, 1s time delay 20% of line impedance reverse reach

Zone 2 is set such that it coordinates with the shortest adjacent line. If this is not taken into account then selective operation can be lost as shown in Figure 2-6. If Z2 of R1 is set such that it covers 50% of the longest adjacent line (dotted line in Figure 2-6), then it would overlap with Z2 of R2 resulting in loss of coordination. As such, Z2 for R1 may trip before Z2 of R2 for a fault between R4 and the end of Z1 of R2 (fault position shown in Figure 2-6). Therefore, the dashed line represents the correct coordinated zone setup.

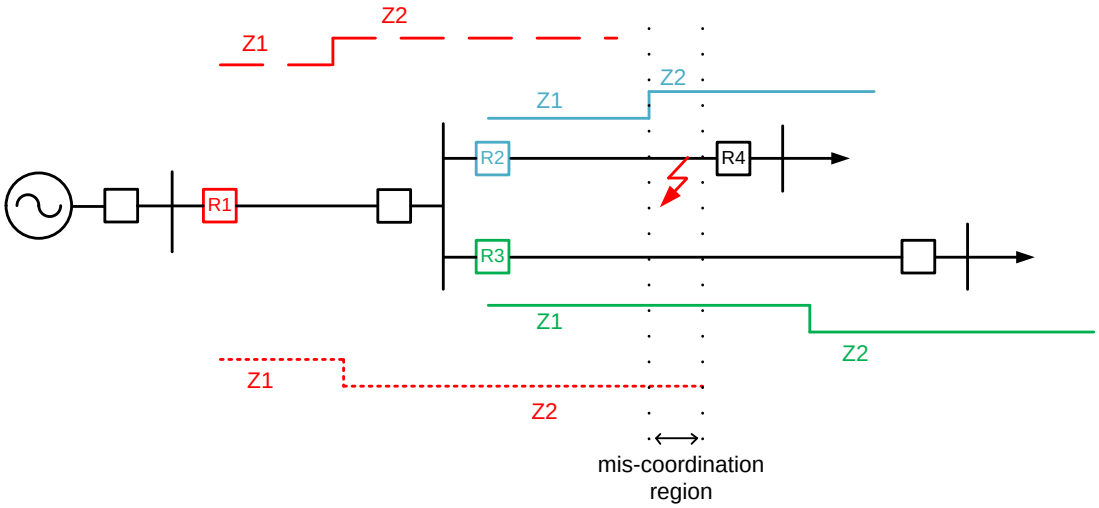

Figure 2-6 Zone 2 coordination with shortest adjacent line

2.3.2 Ground fault detection

Distance protection settings are expressed using positive sequence quantities. Apparent impedance is also calculated in the same manner. Therefore, to accommodate ground faults, a compensation factor k_0 is used in the calculation. This takes into account the ground loop impedance during a ground fault situation. Different relay manufacturers implement this compensation factor in

different ways. Therefore, it is important to refer to the relay documentation to ensure the correct settings of the factor. k_0 for instance is normally calculated using the positive and zero sequence line impedances Z_1 and Z_0 respectively as in (3) [16]:

$$k_0 = (Z_0/Z_1) - 1 \quad (3)$$

Alternatively, a residual compensation factor k_n can be used where $k_n = k_0/3$. In this case, the measured ground fault impedance will depend on the residual current measurement I_n instead of the zero sequence current I_o used in (1) [16].

2.3.3 Communications based distance schemes

The performance of distance protection schemes can be enhanced using communications channels. This is particularly useful in interconnected transmission circuits where faults at certain positions are not immediately cleared by zone 1 elements on both ends. Faster fault clearance times can be achieved through remote signalling. Two commonly used distance schemes are summarised in Table 2-2.

Table 2-2 Common communications based distance schemes and their application [8]

Scheme category	Scheme types	Principle of operation
Transfer tripping	Direct under-reach transfer trip, permissive under-reach transfer trip, permissive over reach transfer trip.	An intertripping signal from the fault detecting end of the line is used to directly trip the remote end of the line to accelerate fault clearance. Additional checks can be applied including remote zone 2 pickup and directional checks.
Overreach blocking	Over reach blocking using zone 1, over reach blocking using zone 2.	Lengthy fault clearance delays can be caused if the communication channel is faulty, so a combination of inverse logic and the pickup of overreaching zones are used.

2.3.4 Distance protection application issues and considerations

Although distance protection is considered a mature protection method, a number of application challenges persist. These are briefly discussed here along with some advances aiming to tackle them.

a) Load encroachment

Load encroachment occurs when the apparent impedance caused by a circuit overload encroaches into the distance protection zones. This usually occurs with long transmission lines whose impedance is comparable to that of the load and is usually accompanied with a voltage depression. Load encroachment into zone 3 was one of the main events leading to the North American blackout in 2003 [18]. Load blinders are usually used to deal with load encroachment. These eliminate the area of the distance characteristic prone to load encroachment as shown in Figure 2-7.

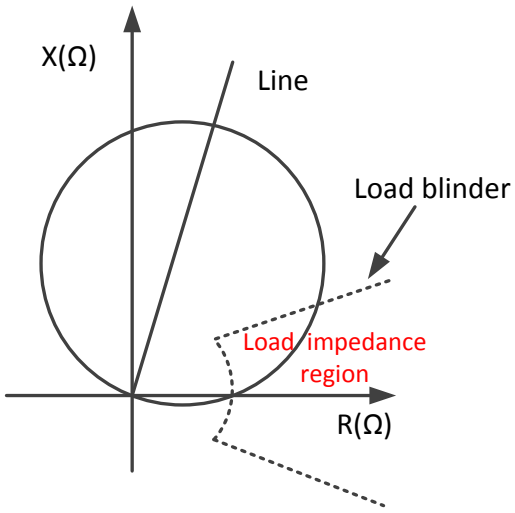

Figure 2-7 Load blinders used to minimise load encroachment

In a piece of work commissioned by NERC [19], it was concluded that if load blinders are used, transmission line loadability can be increased to 150% of the thermal rating while still providing adequate resistive fault coverage.

b) Multi terminal line arrangements

Distance schemes applied to multi-terminal circuit configurations (as shown in Figure 2-8) are particularly challenging [20]. Different source infeeds from the circuit terminals affect the apparent impedance seen by the relay which may cause reach inaccuracies. For example, the fault contribution from the teed circuit for the fault illustrated in Figure 2-8 results in an increase in the apparent impedance measured at R1. Zone 2 set to protect the remote busbar B and beyond would then under-reach [8]. The reach of Zone 2 for R1 can be set to take into account the worst case infeed from the teed feeder. This may result in a large overreach when the infeed is switched off. An under-reach direct transfer trip scheme may also be used [8].

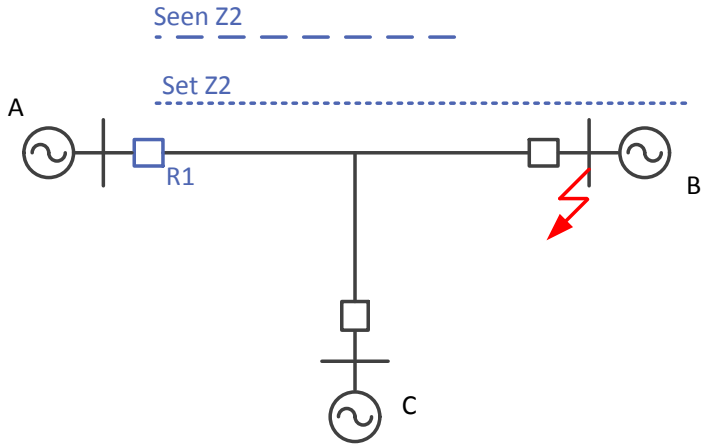

Figure 2-8 Distance protection of multi-terminal circuits

c) Mutual coupling between parallel circuits

Zero sequence mutual coupling between parallel lines during earth faults can result in under-reach [3, 21]. This is particularly problematic with un-transposed lines. This can usually be addressed using additional current inputs from parallel circuits into the distance scheme to compensate for the coupling effect. Additional factors can affect the reach accuracy including earthing arrangements and the earthing or otherwise of de-energised parallel lines. Another compensation technique proposed in literature determines the state of the circuits involved and produces a correction factor accordingly [22].

d) Circuits with Flexible AC Transmission Systems (FACTS)

The connection of FACTS devices (e.g. series and shunt compensation) present a number of challenges, mostly reach related, when setting distance protection relays [23-25]. Transmission system operators usually deal with such problems on a case by case basis with through detailed system studies and manufacturer recommended settings [20]. Some of these issues will be picked up in chapter 3

2.4 DER interface protection

Engineering recommendations such as G59/2 [26] in the UK or IEEE 1547 guidelines [27] stipulate the functions necessary to protect the DER. These differ according to the type of DER, the voltage level it is connected to and the country. [28] provides useful information on international practices related to the protection of DER. This section focuses on loss of mains (LOM) protection functions as it will be revisited in chapter 3.

2.4.1 Loss of mains protection

Loss of mains is the condition where a section of the distribution network is disconnected from the main grid and remains energised by installed DER. This islanded mode of operation is not currently permitted due to the following reasons [29]:

- The islanded distribution network frequency may drift in relation to the main grid. Therefore, out of synch re-closures at the point of common coupling are a possibility unless check synchronism functionality is fitted.
- Power quality usually cannot be maintained by DER.
- Operational procedures normally assume that an islanded network is not energised which if it were not true would pose a safety risk to personnel working on this network.

A surplus or deficit in generation capacity provided by the DER compared to the local load in the islanded network determines the ease of detecting a LOM condition. When these are not matched then voltage and frequency protection can be effectively used to detect LOM [8]. However, when generation and local

loading are closely matched then it is more difficult to detect the islanding event. Therefore, more specialised protection functions are included. The most commonly used functions are rate of change of frequency (ROCOF) and voltage vector shift (VS) [8].

ROCOF as the name suggests monitors variation in system frequency as an indicator for LOM. The rate of change of frequency $\mathrm{d}f/\mathrm{dt}$ can be calculated according to (4) over a three cycle window using measured frequency f_n [30]:

$$\mathrm{d}f/\mathrm{dt} = \frac{f_n - f_{n-3cycle}}{3cycle} \tag{4}$$

ROCOF can suffer from spurious tripping in response to remote disturbances. Such behaviour can lead to undesirable tripping of DER which can exacerbate system frequency disturbances [31]. A number of alternative solutions have been proposed to improve the stability of ROCOF such as CO-ROCOF which relies on communications to enhance the scheme performance [32]. Other communications-based protection algorithms in the research stage rely on internet [33] or satellite [34] communications to provide a reference frequency signal representing the frequency of the grid.

Recent developments, that are undergoing field trials, include the phase angle drift (PAD) algorithm. This LOM protection algorithm relies on historical frequency data and an accumulator which, when it exceeds a pre-set threshold, results in a trip command [35].

2.5 System integrity protection schemes

In addition to the protection against short circuits, there are schemes that are used to protect the overall integrity of the power system against certain events that usually lead to unstable transients, overloads or, in extreme cases, blackouts. These are called system integrity protection schemes (SIPS) [36]. The actions performed by system integrity schemes are designed based on extensive system studies. For example, frequency excursions lasting longer than a predefined amount of time usually trigger generation or load disconnection as appropriate. Failing to do so can result in loss of system synchronism. Similarly,

excursions in voltage limits (usually voltage depression) should be treated to avoid a system voltage collapse. This can be remedied by managing power flows or switching of FACTS [37]. The advent of wide area measurements promises more flexibility in available protection actions through the implementation of more advanced SIPS functions.

2.6 Wide area measurement, protection, automation and control

2.6.1 Synchrophasor measurement technology

Collecting synchronised voltage measurements from remote busses was first discussed in [11]. The technology has since then developed significantly and currently relies on GPS (global positioning system) as a universal source of synchronising signals. These signals are used by phasor measurement units (PMU) to time stamp each measurement made for comparison at a later stage. The operation of PMUs is described in standard IEEE C37.118 [38, 39]. Synchrophasor measurement technology (SMT) consists of a number of building blocks which provide data measurement, collection, archiving and visualisation systems. SMT can be used in a range of applications, mainly in system monitoring where it is usually referred to as a wide area measurement system (WAMS) [40].

A number of real-time protection and control applications based on PMU measurements have been proposed. These, however, require further development and the appropriate infrastructure put in place including suitable communications networks and algorithms. These are usually referred to as wide area measurement protection and control systems (WAMPAC) [40]. Figure 2-9 depicts a typical WAMPAC architecture. An extended version of this architecture can be found in [41], where WAMS can be utilised to perform adaptive protection functions to cope with variable power system operational states.

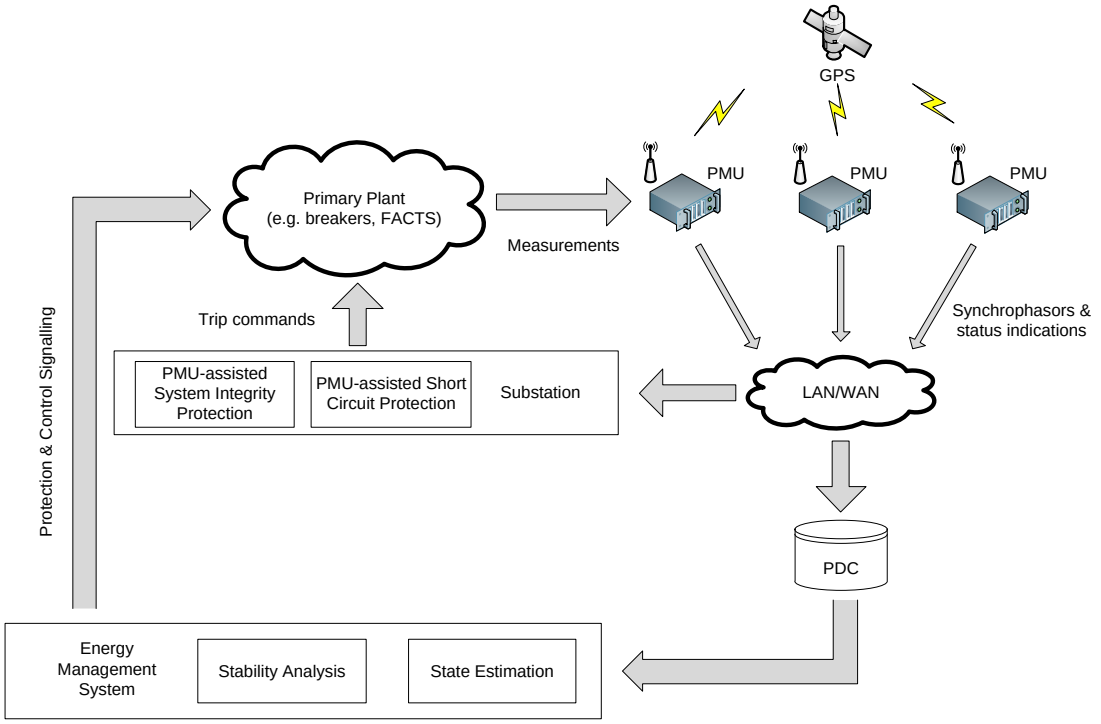

Figure 2-9 Typical WAMPAC architecture

2.6.2 Protection applications of SMT

SMT is seen as an enabler for more advanced system integrity protection functions. The ability to compare measurement from the wider network can enable greater flexibility and potentially more selective protection operation. Below is a list of some SMT based protection functions proposed in the literature [42]:

- Predictive angular and voltage stability protection.
- Fault localisation and classification.
- Precise islanding detection.
- Adaptive load shedding.
- Real-time state measurement or estimation to enable further protection and control functions.

It is envisaged that SMT technology can enhance dependable and secure performance of SIPS. By shifting the balance between these performance criteria when the system is normally loaded or under stress respectively, undesirable operation can be avoided [43].

2.7 The digital substation

The introduction of microprocessor based protection and control devices has enabled the delivery of more powerful and flexible functions. The term digital substation refers to the integration of these devices over communications channels. Intelligent electronic devices (IEDs) are considered the building block of digital substations.

2.7.1 Intelligent electronic devices

Relaying platforms have evolved from electromechanical based protection relays to multifunctional numerical functions implemented on IEDs. The latter offers a wide range of protection functionality within a single physical device along with more integration of monitoring and control functions.

2.7.1.1 IED advantages over legacy relaying platforms

Greater flexibility in protection scheme deployment is achieved due to a potentially large number of protection and automation functions that can be activated on any given IED. IEDs are based on embedded platforms that constitute modular hardware components. This means that upgrading a scheme's I/O or hardware capabilities is a relatively straightforward task since complete hardware replacement is not necessary. Upgrades to the functionality can also be achieved through firmware upgrades. Figure 2-10 shows a typical hardware architecture of a modern IED [8, 10].

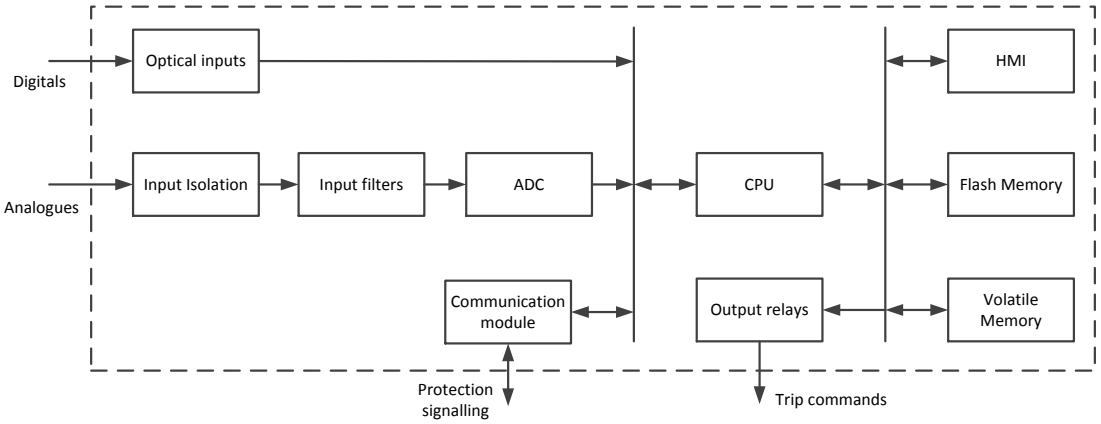

Figure 2-10 IED hardware architecture

The use of a numerical platform allows the use of advanced measurement techniques including adaptive digital filtering and adaptive frequency tracking. Consequently, protection algorithms can be more immune to adverse conditions such as harmonics. Furthermore, reliable operation can be maintained even at off nominal system frequencies [44]. Digital fault and event recording are standard features in protection IEDs. These enable the performance of post fault diagnostics to verify relay operation. IED now also integrate PMU measurement capabilities, a testament of a highly integrated and powerful substation automation platform.

The ability to communicate remotely with IEDs is perhaps one of the most compelling benefits of the platform. Not only does this allow the remote interrogation of the relay status including the extraction of fault records, but it also allows remote configuration of the relay including the adjustment of its settings.

Programmable scheme logic (PSL) is another useful feature of numerical relays. Device I/O in addition to internal function I/O can be mapped to a user specified logic diagram. This allows greater control over the behaviour of protection in more complex schemes. Flexibility in operation can also be achieved by specifying additional logic inputs to a protection element which contribute in determining the final state of the relay output (e.g. trip command). Figure 2-11 shows a snapshot of a PSL taken from a commercial relay configuration software (ALSTOM's MiCOM S1 Agile [45]).

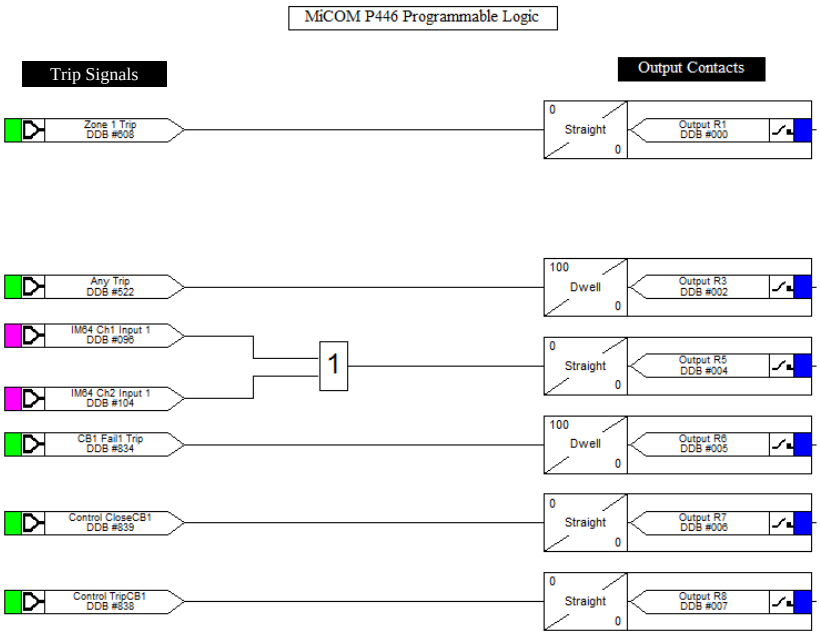

Figure 2-11 Typical PSL diagram [45]

2.7.1.2 IED reliability

IEDs have built in features that enhance their reliability. For instance, the overall health of the hardware and software execution is monitored using watchdog functions and checksums [8]. These self-supervision features allow early detection of IED or auxiliary system faults by raising appropriate alarms. As a result, the mean time to repair (MTTR) is significantly reduced compared to standard maintenance cycles (1-5 years). Consequently, higher relay availability is achieved [46]. I/O supervision including current transformer (CT), voltage transformer (VT) and trip circuit supervision are also standard features of IEDs. Faults in any of these components can be identified and reported.

IEDs also employ security measures such as multi-level password protection to prevent unauthorised access to the devices and unapproved changes in their configuration. These are important cyber security features as modern substations become increasingly accessible remotely and reliant on mainstream ICT technologies.

2.7.2 IEC 61850 communications standard

Proprietary communications protocols are very common among protection devices. This impeded further integration between devices from different manufacturers. Greater interoperability was desired by utilities such that scheme replacement costs are minimised and its process simplified. The IEC 61850 is a standard for communications networks and systems in substations [47]. It aims to enable interoperability between devices from different manufacturers by specifying a data model and a mapping between the model and the underlying mainstream communications stack to perform required data exchange services.

IEC 61850 emphasises functional abstraction by utilising the so called logical nodes (LN). Substation automation functions are decomposed into LNs which reside in physical devices (PD). LNs are effectively containers of data objects (DO) which can be exchanged between devices from different vendors. This hierarchy is illustrated in Figure 2-12.

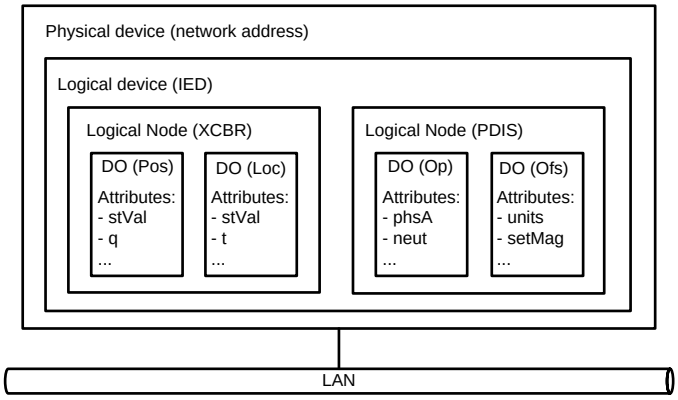

Figure 2-12 IEC 61850 functional hierarchy

A typical substation architecture employing IEC 61850 is depicted in Figure 2-13. The process bus is where measurement and control commands are exchanged in a digital format. Analogue measurements are digitised using merging units (MU) or NCITs and are transferred across the process bus at a high rate using sampled values (SV), the format of which is specified in the standard. This allows the sharing of measurements between different devices without the need for dedicated hardwiring between transducers and relays.

This provides significant cost savings in wiring. Measurement circuit redundancy can still be achieved by configuring the process bus in a ring arrangement. Tripping signals are exchanged using high speed GOOSE (generic object oriented substation event) messages. The station bus interconnects the protection and control bays with substation gateways and human machine interfaces (HMI). The nature of the communications at the station bus means they are not as time critical as those at the process bus and follows a client-server approach. Data related to fault records and alarms are transferred across the station bus.

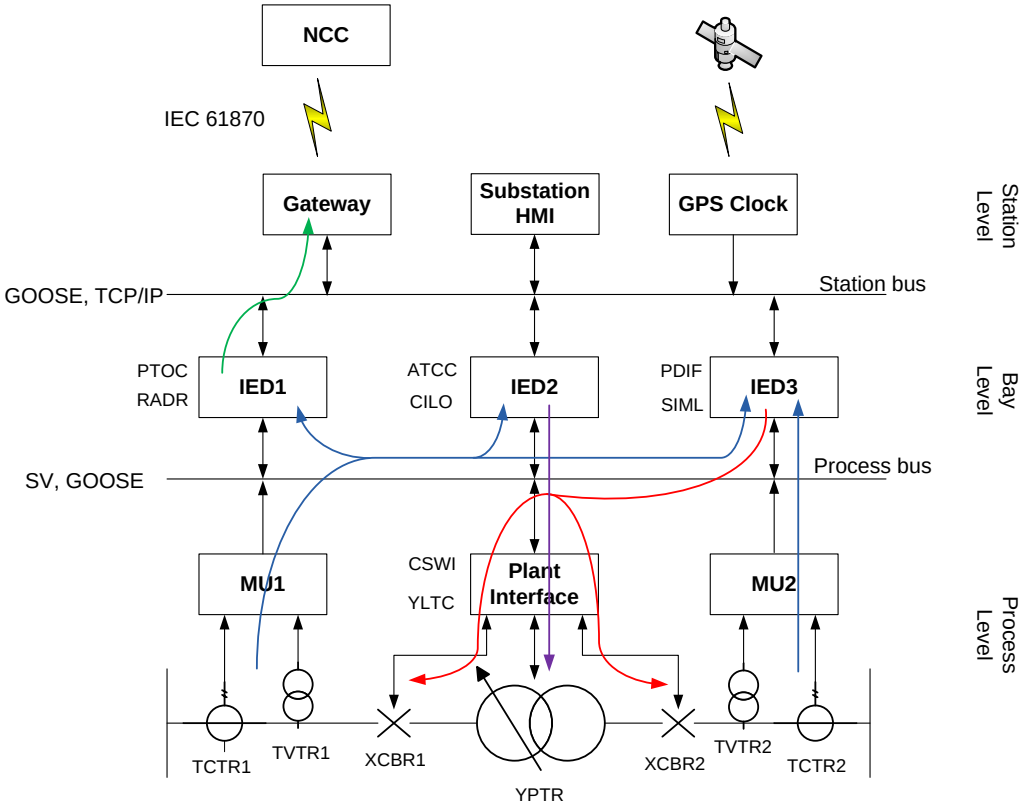

Figure 2-13 Typical substation architecture utilising IEC 61850

The level of interoperability achieved can only be as robust as the tools used to configure the substation automation system. An XML based substation configuration language (SCL) is specified in the standard. Engineering tools from different vendors can produce and make use of files to configure protection devices from different manufacturers. The files used contain

information about the capabilities of the IEDs in the substation, their connectivity and the configuration of the primary system such as voltage levels.

2.8 Functional testing of power system protection

The testing of protection devices is important to ensure that they are capable of delivering the performance levels necessary for a safety critical application. There is a wide range of tests that are conducted by relay manufacturers and utilities and these are covered by international standards and testing procedures. The tests cover environmental, mechanical, electrical and functional aspects of the devices under test (DUT). This section will focus on functional testing since it will be revisited at a later stage in this thesis. Information on other types of tests can be found in [8].

2.8.1 Functional type testing

Functional type testing involves applying appropriate inputs to the DUT and measuring the performance of the relay in response to these inputs. This is then verified against specifications described in international standards such as IEC 60255 [48]. For instance, a standard inverse IDMT overcurrent protection element can be subjected to simulated short circuit currents, through secondary injection, to verify that the characteristic does indeed comply with the IEC 60255 IDMT specifications in terms of operating times, pick up and drop off thresholds, accuracy limits, etc.

2.8.1.1 Static type testing

Secondary injection test amplifiers are used to apply inputs to the DUT and record their response. These are usually connected to a host PC with appropriate control software that automatically applies these tests.

2.8.1.2 Dynamic type testing

Dynamic type tests involve the use of a power system simulator to generate the input testing signals as well as receive the trip commands from the DUT. Nowadays, digital power system simulators are used to model the protected primary systems to a high fidelity. Analogue outputs can be reproduced faithfully and even contain high frequency information if necessary. These

simulators are equipped with analogue and digital I/O to interface with the DUT. Dynamic type tests are automated where the response of the DUT is recorded for later analysis and verification. Modern simulators also offer communications based interfaces such as IEC 61850 SV and GOOSE inputs and outputs. This enables the testing of relays compliant with the standard. Figure 2-14 shows a schematic of a dynamic type testing arrangement.

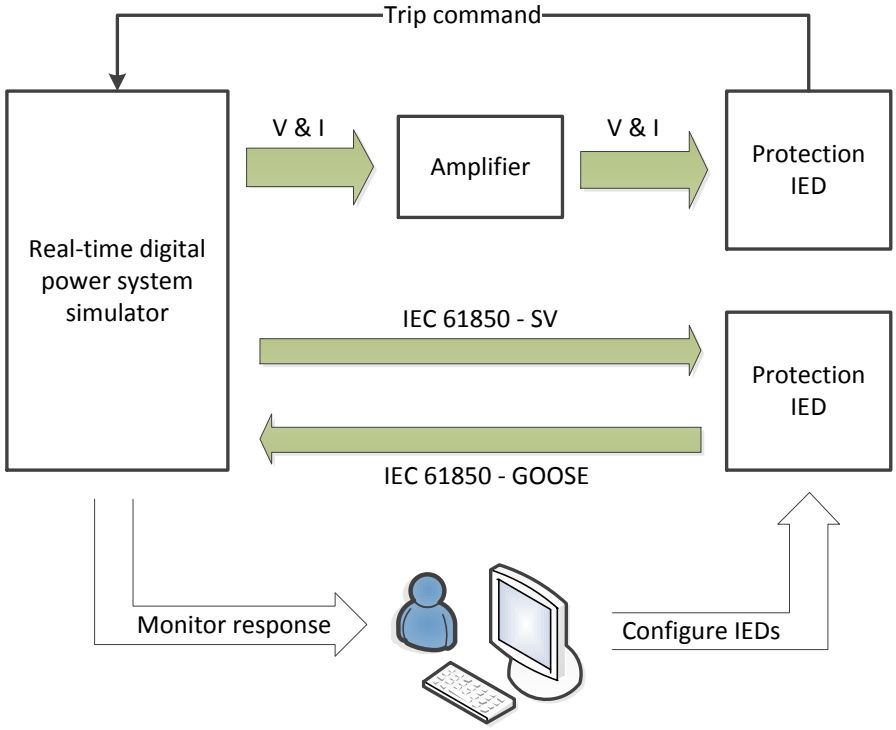

Figure 2-14 Dynamic type testing of protection relays

2.8.2 Software type testing

Software used to implement the protection functions must be tested thoroughly. This aims to ensure that software elements are error free and do not contain flaws in data structures or logic. Unit testing of software functions is performed to verify these functions against the software specification detailed by the manufacturer. The integration of different software elements is also tested to ensure that the software interfaces comply with the specification. Dedicated automated software testing tools are used for this purpose to ensure consistency in testing results. The integration between software and hardware

is also tested. In this case, the operation of low level drivers is verified along with execution timings, I/O, etc [8].

2.8.3 Commissioning testing

When a protection scheme is deployed in the field, a whole host of tests are conducted to ensure correct scheme connectivity, configuration and functionality. On site secondary and primary injection are conducted. The correct operation of the scheme is determined while at the same time ensuring that instrument transformer connections are also correct [8].

2.8.4 Shortfalls of existing testing practices

The testing practices described above are suitable for existing applications and protection functions. However, as new developments in power system protection are introduced, new and improved testing procedures may be necessary [49]. Such changes include:

- Introduction of adaptive protection functions.
- Further integration between protection and control functions.
- Protection functions become more reliant on communications.

Lack of testing standards to deal with some of these changes is one of the main issues. Existing standards may not need to be replaced, but they can certainly be complemented to accommodate new functions and substation configurations. The aforementioned changes introduce an additional layer of variable performance that must be verified prior to deployment.

To this end, a comprehensive suite of tests may need to be devised in order to deal with emerging changes in protection practices. If more complex functions are to be deployed, then the utilities will have less visibility of the intricacies of the scheme. Therefore, it is necessary to develop accessible tools for the protection engineers. It may then be necessary to provide more contextual information about test configurations and test reports. For instance, instead of having to deal with low level protection scheme configuration, a user may select test scenarios customised for a certain power system operating condition. The

test system would then select the appropriate scheme configuration and test scenarios to verify the required functionality.

Conventional testing practices of wide area protection schemes may prove difficult. For instance, planning outages for several substations involved in a WAMPAC scheme for commissioning is impractical. Therefore, alternative means of testing may be necessary. Perhaps more emphasis should be placed on offsite verification procedures.

2.9 Chapter summary

The art and science of protective relaying continues to evolve. New functional and performance requirements emerge to achieve greater integration and to address some performance issues. One of the most important features of power system protection in the past decade is the push for device interoperability and more reliance on communications networks.

This chapter reviewed some of the fundamentals of power system protection while emphasising distance and LOM protection as they will be revisited in later chapters. Recent system blackouts have stimulated a lot of activity in wide area protection schemes in an attempt to devise protection functions which minimise erroneous behaviour under stressed system conditions and even avoid unstable transients.

The testing of new protection devices has also seen major steps forward especially with modern IEDs. However, as new functions emerge especially those dealing with wide area phenomena, testing requirements must be revised. Furthermore, new tools may be necessary to deal with some of the complex configurations of new protection schemes.

2.10 References

[1] B. M. Weedy and B. J. Cory, *Electric power systems*: Wiley, 1998.

[2] IEEE, "IEEE Std C37.113-1999: IEEE Guide for Protective Relay Applications to Transmission Lines," ed, 2000.

[3] P. M. Anderson, *Power System Protection* Wiley-IEEE Press, 1999.

[4] A. Dysko, G. M. Burt, S. Galloway, C. Booth, and J. R. McDonald, "UK distribution system protection issues," *Generation, Transmission & Distribution, IET,* vol. 1, pp. 679-687, 2007.
[5] M. A. Zamani, T. S. Sidhu, and A. Yazdani, "A Protection Strategy and Microprocessor-Based Relay for Low-Voltage Microgrids," *IEEE Transactions on Power Delivery,* vol. 26, pp. 1873-1883, 2011.
[6] F. Coffele, C. Booth, G. Burt, C. McTaggart, and T. Spearing, "Detailed Analysis of the Impact of Distributed Generation and Active Network Management on Network Protection Systems," in *CIRED 2011*, 2011.
[7] R. M. Tumilty, M. Brucoli, G. M. Burt, and T. C. Green, "Approaches to network protection for inverter dominated electrical distribution systems," in *Power Electronics, Machines and Drives, 2006. PEMD 2006. The 3rd IET International Conference on*, 2006, pp. 622-626.
[8] Alstom, *Network Protection and Automation Guide - Protective Relays, Measurement and Control*, 2011.
[9] P. Orr, G. Fusiek, C. D. Booth, P. Niewczas, A. Dysko, F. Kawano*, et al.*, "Flexible protection architectures using distributed optical sensors," in *Developments in Power Systems Protection, 2012. DPSP 2012. 11th International Conference on*, 2012, pp. 1-6.
[10] A. T. Johns and S. K. Salman, *Digital Protection for Power Systems*: IEE, 1997.
[11] A. G. Phadke, J. S. Thorp, and M. G. Adamiak, "A New Measurement Technique for Tracking Voltage Phasors, Local System Frequency, and Rate of Change of Frequency," *Power Apparatus and Systems, IEEE Transactions on,* vol. PAS-102, pp. 1025-1038, 1983.
[12] L. Hunt, "Drivers for packet-based utility communications networks-teleprotection," in *Advanced Power System Automation and Protection (APAP), 2011 International Conference on*, 2011, pp. 2453-2457.
[13] M. Ojaghi, Z. Sudi, and J. Faiz, "Implementation of Full Adaptive Technique to Optimal Coordination of Overcurrent Relays," *Power Delivery, IEEE Transactions on,* vol. 28, pp. 235-244, 2013.
[14] G. Ziegler, *Numerical Distance Protection: Principles and Applications*, 4th ed.: Wiley, 2008.
[15] B. Kasztenny and D. Finney, "Fundamentals of Distance Protection," in *Protective Relay Engineers, 2008 61st Annual Conference for*, 2008, pp. 1-34.
[16] Verzosa, Jr., "Ground Distance Relays - Understanding the Various Methods of Residual Compensation, Setting the Resistive Reach of Polygon Characteristics, and Ways of Modelling and Testing the Relay," *PACWorld*.
[17] S. Jamali and H. Shateri, "Robustness of Distance Relay with Quadrilateral Characteristic against Fault Resistance," in *Transmission and Distribution Conference and Exhibition: Asia and Pacific, 2005 IEEE/PES*, 2005, pp. 1-6.
[18] US.-Canada Power System Outage Task Force, "Final Report on the August 14th Blackout in the United States and Canada," 2004.
[19] NERC, "Increase Line Loadability by Enabling Load Encroachment Functions of Digital Relays," 2005.

[20] CIGRÉ. W.G. B5.15, "Modern Distance Protection Functions and Applications," 2008.
[21] K. R. Pillay and B. S. Rigby, "Studying the impact of mutual coupling on distance protection relays using a real-time simulator," 2011, pp. 1-6.
[22] M. Sanaye-Pasand and P. Jafarian, "An Adaptive Decision Logic to Enhance Distance Protection of Transmission Lines," *IEEE Transactions on Power Delivery,* vol. 26, pp. 2134-2144, 2011.
[23] M. Khederzadeh and T. S. Sidhu, "Impact of TCSC on the protection of transmission lines," *Power Delivery, IEEE Transactions on,* vol. 21, pp. 80-87, 2006 2006.
[24] T. S. Sidhu, R. K. Varma, P. K. Gangadharan, F. A. Albasri, and G. R. Ortiz, "Performance of distance relays on shunt-FACTS compensated transmission lines," *Power Delivery, IEEE Transactions on,* vol. 20, pp. 1837-1845, 2005 2005.
[25] I. F. Abdulhadi, G. M. Burt, A. Dysko, R. Zhang, and J. Fitch, "The evaluation of distance protection performance in the presence of Quadrature Boosters in support of a coordinated control strategy," in *Developments in Power System Protection (DPSP 2010). Managing the Change, 10th IET International Conference on*, 2010, pp. 1-5.
[26] Electricity Networks Association, "ER G59/2: Recommendations for the Connection of Generating Plant to the Distribution Systems of Licensed Distribution Network Operators," 2010.
[27] IEEE, "IEEE Application Guide for IEEE Std 1547, IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems," 2009.
[28] CIGREÉ. W.G. B5.34, "The Impact of Renewable Energy Sources and Distributed Generation on Substation Protection and Automation," 2009.
[29] I. Abdulhadi, X. Li, F. Coffele, P. Crolla, A. Dysko, C. Booth*, et al.*, "International White Book on DER Protection: Review and Testing Procedures," 2012.
[30] Alstom, *MiCOM P341 Interconnection Protection Relay Technical Manual*: Alstom Grid, 2011.
[31] NGET, "Report of the national grid investigation into the frequency deviation and automatic demand disconnection that occured on the 27th May 2008," 2009.
[32] C. G. Bright, "COROCOF: comparison of rate of change of frequency protection. A solution to the detection of loss of mains," in *Developments in Power System Protection, 2001, Seventh International Conference on (IEE)*, 2001, pp. 70-73.
[33] D. Laverty, D. J. Morrow, and T. Littler, "Internet based loss-of-mains detection for distributed generation," in *Universities Power Engineering Conference, 2007. UPEC 2007. 42nd International*, 2007, pp. 464-469.
[34] A. Dysko, G. M. Burt, P. J. Moore, I. A. Glover, and J. R. McDonald, "Satellite Communication Based Loss-of-Mains Protection," in *IET 9th International Conference on Developments in Power System Protection, 2008. DPSP 2008*, 2008, pp. 687-692.

[35] H. T. Yip, G. Millar, G. J. Lloyd, A. Dysko, G. M. Burt, and R. Tumilty, "Islanding detection using an accumulated phase angle drift measurement," in *Managing the Change, 10th IET International Conference on Developments in Power System Protection (DPSP 2010)*, 2010, pp. 1-5.
[36] M. Begovic, V. Madani, and D. Novosel, "System Integrity Protection Schemes (SIPS)," in *2007 iREP Symposium - Bulk Power System Dynamics and Control - VII. Revitalizing Operational Reliability*, 2007, pp. 1-6.
[37] N. R. Chaudhuri, A. Domahidi, R. Majumder, B. Chaudhuri, P. Korba, S. Ray*, et al.*, "Wide-area power oscillation damping control in nordic equivalent system," *IET Generation, Transmission Distribution,* vol. 4, pp. 1139-1150, 2010.
[38] IEEE, "IEEE Std C37.118.1-2011: IEEE Standard for Synchrophasor Measurements for Power Systems," ed, 2011, pp. 1-61.
[39] IEEE, "IEEE Std C37.118.2-2011: IEEE Standard for Synchrophasor Data Transfer for Power Systems," ed, 2011, pp. 1-53.
[40] M. G. Adamiak, A. P. Apostolov, M. M. Begovic, C. F. Henville, K. E. Martin, G. L. Michel*, et al.*, "Wide Area Protection—Technology and Infrastructures," *Power Delivery, IEEE Transactions on,* vol. 21, pp. 601-609, 2006.
[41] V. Terzija, P. Regulski, L. P. Kunjumuhammed, B. C. Pal, G. Burt, I. Abdulhadi*, et al.*, "FlexNet wide area monitoring system," in *2011 IEEE Power and Energy Society General Meeting*, 2011, pp. 1-7.
[42] V. Terzija, G. Valverde, C. Deyu, P. Regulski, V. Madani, J. Fitch*, et al.*, "Wide-Area Monitoring, Protection, and Control of Future Electric Power Networks," *Proceedings of the IEEE,* vol. 99, pp. 80-93, 2011.
[43] E. E. Bernabeu, J. S. Thorp, and V. Centeno, "Methodology for a Security/Dependability Adaptive Protection Scheme Based on Data Mining," *IEEE Transactions on Power Delivery,* vol. PP, pp. 1-1.
[44] D. Tholomier and A. Apostolov, "Adaptive protection of transmission lines during wide area disturbances," in *Power Systems Conference and Exposition, 2009. PSCE '09. IEEE/PES*, 2009, pp. 1-7.
[45] AREVA, *MiCOMho P445 and P446 Fast Multifunction Distance Protection: Technical Manual*, 2007.
[46] ABB, *Self supervision techniques, 670 series Principles and functions*: ABB, 2009.
[47] IEC, "IEC 61850: Communication networks and systems in substations," ed, 2003.
[48] IEC, "IEC 60255: Measuring relays and protection equipment," ed, 2010.
[49] I. Abdulhadi, F. Coffele, A. Dysko, C. Booth, G. Burt, G. Lloyd*, et al.*, "Performance Verification and Scheme Validation of Adaptive Protection Schemes," in *2012 CIGRÉ Session (44th Edition)*, 2012.

3 Evaluating the Performance of Existing Protection Schemes under Flexible Primary System Operation

3.1 Chapter methodology and contributions

Protection scheme performance is increasingly suffering due to the influence of primary and secondary system conditions and defects respectively, with varying impact, and it is important to provide flexibility in protection behaviour in order to cope with such deterioration in performance. This is the underlying hypothesis of the chapter which requires understanding the nature of the conditions affecting the performance of protection schemes and demonstrating their impact. This consequently enables assessing the appropriateness of flexible protection scheme behaviour as a means of enhancing their performance.

The previous chapter reviewed power system protection and its importance to system integrity. It also included recent developments in protection schemes and digital substations which increasingly make use of communications channels. Furthermore, the chapter also highlighted some of the most recent changes and improvements made in certain protection schemes to cope with changes in the primary system either due to common use of FACTS (or similar devices), more frequent changes in network topology, wide-area disturbances and increased utilisation of DER.

This chapter therefore reviews the impact these changes have on existing protection schemes as well as the potential impact future trends in power system operation have on the performance of these schemes. This review specifically qualifies the impact these have on protection from the point of view of flexible power system operation which is becoming an increasingly common

approach to operating a stressed primary system while minimising major reinforcements. By understanding the nature of the impact these system changes have, opportunities for improving the performance of protection schemes can be duly identified. The provision of sought after improved performance is argued to be through striking a balance between robust and flexible protection scheme behaviour.

Detailed simulations have been conducted in this chapter to illustrate the shortfalls in protection performance in two example cases – distance protection and loss of mains protection. Protection sensitivity and stability evaluation have been conducted on the former to ascertain the impact of different DER operating conditions, coupled with islanding and remote disturbances, on the performance of loss of mains protection. The latter evaluates reach selectivity of distance protection while quadrature booster transformers exist and are actively managed on the protected or adjacent circuits. Both studies conducted were unique at the time of writing the thesis in terms of primary system operating conditions and thoroughness of simulations and protection performance testing.

The main contributions of this chapter are:

- Reviews the impact topology changes, DER utilisation, FACTS and wide-area disturbances have on protection performance. These factors have also given impetus to the flexible operation of the primary system, and consequently the impact that has on protection performance was also examined. The latter examination was unique at the time of writing the thesis.
- Quantification through simulation of QB impact on the reach of distance protection zones 2 and 3 under all possible QB operating modes and different fault conditions. This exercise also qualifies the additional potential reach issues that coordinated QB control can pose. Particularly under coordinated QB control, the National Grid UK recommended distance protection settings are shown to be potentially exposed.

- Quantification through secondary injection of loss of mains protection sensitivity and stability under a comprehensive set of testing scenarios and using commercial relaying products. This also revealed the disparity of performance between different LOM protection offerings under the same operating conditions due to different LOM algorithm implementations. Moreover, compromise settings are proposed along with LOM protection performance evaluations procedures and were recommended for industry use.
- Argues the necessity of protection to exhibit both robust and flexible behaviour to achieve improved performance levels especially under flexible power system operation. The balance between these two is defined based on network conditions and protection scheme elements.

3.2 Causes of deterioration in protection performance under flexible power system operation

This section focuses on the impact that flexible operation of power systems can have on the performance of protection schemes. This is in contrast to the available research work which mainly focuses on the impact of discrete primary system components such as DER and FACTS on the performance of existing protection. It is firmly believed that operating a number of these discrete elements to support a flexible power system can reveal new protection performance challenges. Therefore, it is important to outline the additional complexity of operating a primary system in a flexible fashion relative to the traditional operational practices. Consequently, the nature of the impact this can have on protection performance can be understood.

3.2.1 Flexible operation of the primary power system

Increasing pressure to meet renewable generation targets and at the same time maintaining or improving supply security levels present great technical challenges from the operational point of view. This is especially the case when minimising investment cost is a priority constraint. Better utilisation of the existing assets, therefore, becomes more preferable. And achieving this improved utilisation can be partly delivered through flexible operation (in addition to other strategies such as asset life extension which is out with the scope of this thesis). The flexible operation of the primary system entails secondary system strategies (control and protection) which contextually manage constraints to ensure minimum performance levels are not compromised. This research has identified four main areas that can pose a performance penalty on protection systems when the primary system is operated under certain conditions, these are:

- Power system topology changes.
- Utilisation of DER.
- FACTS and similar devices providing operational support.
- Wide-area disturbances.

Some of these areas are well understood and their impact on protection performance has been covered extensively in literature. However, operating the primary system in a flexible fashion may intentionally invoke the increased utilisation of some of these as assets to enable such operation to increase stability margins or improve supply reliability (e.g. FACTS and intentional topology changes). On the flip side, more utilisation of DER and increasingly complex control and protection structures may lead to reduced resilience to severe disturbances due to reduced system inertia or secondary system failure respectively. These are issues that are presenting themselves time and time again when blackouts/brownouts are becoming more commonplace [1, 2].

To this end the aforementioned four distinct areas will be examined to qualify the impact these have on the primary system when it is operated in a flexible manner. And consequently, any adverse effects this can have on the performance of prevailing power system protection practices.

3.2.2 Power system topology changes

Operating the primary system flexibly is usually synonymous to modifying its topology as and when required to fulfil operational objectives a rigid topology cannot achieve. Topology changes considered here include any switchgear controlled modifications to the primary system impedance or power flow paths and these include:

- Shifting of normally open points in a radial distribution network [3].
- Creation of an islanded section of the power system or the splitting of transmission system zones [4].
- Removal of system earthing such as the disconnection of earthing transformers [5].

Some of these topology changes are becoming widespread and more frequent (at least at distribution level) as more automation and active network management schemes are introduced to the system [6]. [7] shows how employing automatic load restoration schemes can affect the performance of overcurrent relays which leads to non-selective operation and the potential for

unnecessary loss of customer supplies. This means that existing distribution protection schemes' performance can be highly susceptible to system topological changes.

System islanding whether used to protect against system collapse, or to facilitate security of supply through micro-grids, is becoming a favourable system operation strategy and policies are emerging to support such operational objective. Intentional islanding, however, brings along with it a whole host of protection performance issues including reliable LOM detection [8, 9] and the lack of sufficient fault contributions for proper protection operation [10, 11].

Changes in the source impedance or ground sources can affect the fault characteristics which can lead to distance protection operation issues [12]. Reach issues are also associated when multiple fault in-feeds are present especially in a teed feeder [13]. However, as more frequent topological changes occur, compromise distance settings may no longer provide the required level of selectivity.

From the above, it can be seen that changing the system topology to meet operational objectives in a flexible manner results in deterioration in protection performance due to:

- Alteration of normal grading paths which affects protection coordination.
- Alteration of fault levels including earth fault contribution which desensitises protection leading to operation failures or reduced coordination.

This highlights the difficulties in meeting stringent protection performance requirements when static settings or protection configuration are employed. Therefore performance levels offered by compromise protection settings usually drop when primary system flexibility through topology changes is adopted.

3.2.3 Utilisation of DER

The increased installed DER capacity and utilisation of DER are seen as one of the main participants in flexible power system operation. Increased penetration of DER in the distribution and transmission networks is changing the passive nature of the primary system. These are less predictable in terms of the power flows and fault level contributions in steady state and transient conditions respectively compared to conventional large scale generation. As discussed previously, intentional islanding can cause operational issues. This is particularly an issue with inverter-interfaced DER. Improved control schemes are proposed to flexibly manage the DERs impact on power system stability and overall quality of supply. These result in an increasingly dynamic DER portfolio where DER connections, composition and configuration change to serve operational objectives and hence result in varying the fault contributions which affect the protection performance [14-16]. To this end, the potential for protection performance deterioration caused by DER is a result of:

- Desensitising of protection due to overall low fault contributions under islanded conditions.
- Mis-coordination of protection due to uncertainty in fault contributions.

Once again, these issues highlight the adverse impact that flexible operation of the primary system has on adopted static protection setting philosophies.

3.2.4 FACTS and similar devices providing system operational support

FACTS such as series compensation and phase shifting transformers as well as similar devices such as fault current limiters aid in increasing the utilisation of the primary system and deferring costly reinforcement as it moves closer to capacity and stability limits. To serve the philosophy of flexible primary system operation, these can be controlled dynamically to meet operational objectives as system constraints change with changing generation profiles, post-fault system configuration and mitigating the effects of severe disturbances. FACTS have been shown to have undesired effects on transmission system protection performance especially in terms of distance reach [17, 18], directional

sensitivity [19] and zone coordination [20]. To a lesser extent, differential protection's harmonic restraint functionality is also affected [21]. Operating these devices dynamically causes further uncertainty in protection performance [17].

Although advanced numerical protection algorithms with dynamic characteristics that aim to compensate for the effects of FACTS are in use [22], a main barrier against reliable performance is the static settings adopted by existing protection schemes.

Fault current limiters (FCL) are another example of how such devices affect the performance of protection schemes. The lower fault levels as well as the additional resistance introduced to the network results in slower overcurrent protection operation and distance protection under-reach respectively [23, 24]. Switching FCLs in and out of a circuit as and when required can prove even more detrimental to a protection scheme applying a fixed setting strategy.

3.2.5 Wide-area disturbances

Reduced system inertia and suboptimal control and protection schemes coupled with a primary system operating at its limits, meant that severe disturbances can have devastating effects often manifesting themselves in wide scale blackouts [25]. The recently frequent occurrence of such disturbances provided impetus for introducing measures to increase system resilience against these disturbances [26] – one of which is flexible primary system operation which introduces its own issues as discussed above.

3.2.6 Hidden failures

Although strictly related to the protection scheme, networks operating at their limits unearth more protection hidden failures. These are system or configuration defects in the protection scheme which only manifest themselves during an event with undesirable consequences [27]. Faulty instrument transformers, incorrectly configured primary/secondary ratios or incorrectly set timers are example hidden failures that can lead to protection mal-operation [28]. Most of these can be attributed to lapses in commissioning protection

system commissioning procedure. Failing to detect these failures is also partly due to the unavailability of continuous platform health checks that can contextually verify the applied protection configuration in addition to standard procedural hardware/software execution checks carried out by relay watchdogs [29]. When the primary system's flexible operation presents protection schemes with variable conditions, dormant hidden failures will almost always present themselves and sometimes with catastrophic consequences.

3.2.7 Closing discussion on performance issues

Inherent to the shortfall in protection performance, are the elements that the protection system constitutes. That is the protection characteristic, scheme logic and to a lesser extent the input stage of the protection. The first two have the protection settings in common. While the protection characteristic is directly affected by the settings, scheme logic is only partially affected by the settings. And as revealed by the review so far, the potentially poor performance is attributed to (from the protection point of view) to unsuitable pick-up thresholds, non-optimal time delays or ineffective signalling.

In order to achieve improved performance, it only makes sense to target these affected elements and seek to modify their behaviour as dictated by the power system conditions.

3.3 Overview of quadrature booster transformers

Quadrature booster transformers (QB) are a special kind of phase shifting transformers (PST) which provide an active means of controlling the power flow in a transmission system where otherwise circuit impedance would passively determine the flow. This is achieved through artificially introducing a phase shift in the voltage angle across the transmission circuit. This is particularly useful to alleviate thermal or stability constraints of heavily loaded transmission networks [30]. QBs are more cost effective compared to PSTs due to the relatively limited range of phase shifting they can provide which is deemed appropriate in certain transmission networks (e.g. UK National Grid) [31].

3.3.1 QB construction, connection arrangements and functions

A QB consists of two sets of windings – shunt and series as shown in Figure 3-1. The shunt element taps the transmission line's phase voltage. This is then shifted by 90˚ and is then injected to the other back to the transmission line through the series element. Figure 3-2 illustrates the voltage phasors associated with the QB and transmission line.

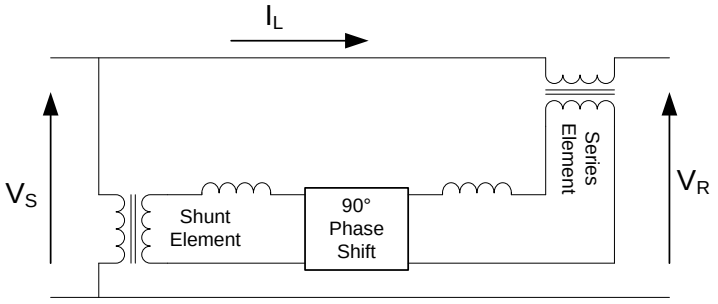

Figure 3-1 Schematic showing QB shunt and series elements

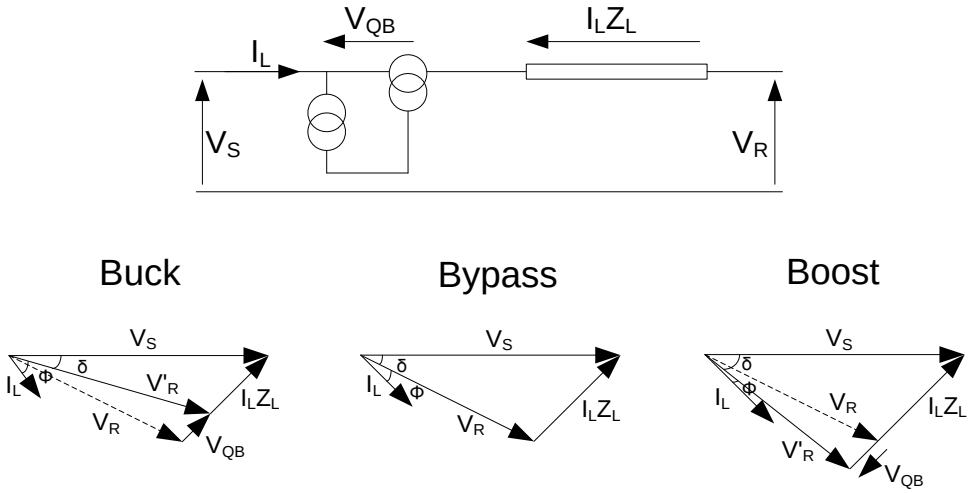

Figure 3-2 QB phasor diagram showing primary system quantities incorporating QB action

The shunt element of the QB is tapped using an on-load tap changer (OLTC) in order to control the voltage magnitude injected into the transmission line by the series elements. This directly controls the phase angle shift introduced by the QB and hence the amount of power flow control in the circuit. There are typically twenty tap positions to provide a maximum phase shift of around 11˚ across the transmission line or around 20% of the MVA rating of the QB [31]. QBs can be found in up to 2750MVA rating which is limited by OLTC rating [32].

Furthermore, the QB operates in two modes – boosting and bucking. When the QB is connected with the shunt element is on the substation busbar side and series element on the transmission line side, boosting mode pushes more power away from the substation and bucking mode impedes the power flow into the transmission line. The tapping convention adopted by UK National Grid denotes tap 1 for maximum boost, tap 39 for maximum buck while centre tap resides at tap 20. Figure 3-3 depicts how a QB is typically connected in a substation. The QB can be bypassed through dedicated switching arrangements for operational or maintenance reasons. The instrument transformers used for protecting the circuit directly connected to the QB are positioned on the transmission line end of the QB. This avoids undesired effects the QB has on the line protection, especially distance protection, which will be apparent from the analysis to follow in section 3.4.

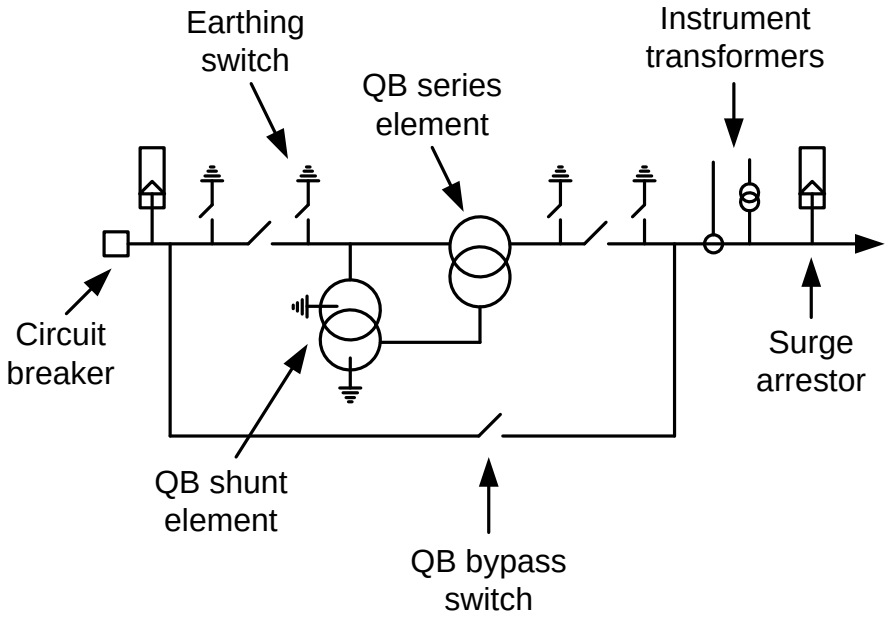

Figure 3-3 QB substation connection arrangement [33]

3.3.2 QB control and protection arrangements

The main function of the QB control system (QBCS) is to set the tap position of the QB based on two factors [31]:

- Tap position selected remotely by the EMS operator.
- QB operating envelope to avoid over-fluxing.

The transmission system operator will seek to choose an optimum setting to control the power flow through constrained circuits. This is particularly important for post-fault management of the system. However, the QB will have a maximum capability due to transformer thermal limits and the potential to over-flux the core especially in bucking mode. Figure 3-4 shows a typical operating envelope at different tap positions that is specified by the QB manufacturer. Thus the QBCS employs this to restrict the tap position should the operating limits be violated. Figure 3-5 shows a high level functional block diagram of a QBCS which uses measured primary quantities in association with the QB operation envelope to enable or restrict tap changes selected by the system operator. The QBCS also performs temperature monitoring and QB data logging.

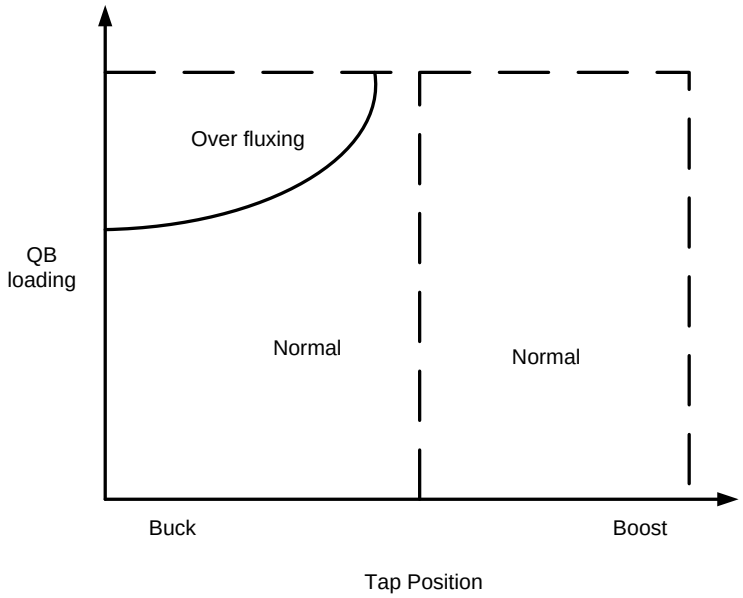

Figure 3-4 Typical QB operating envelope [33]

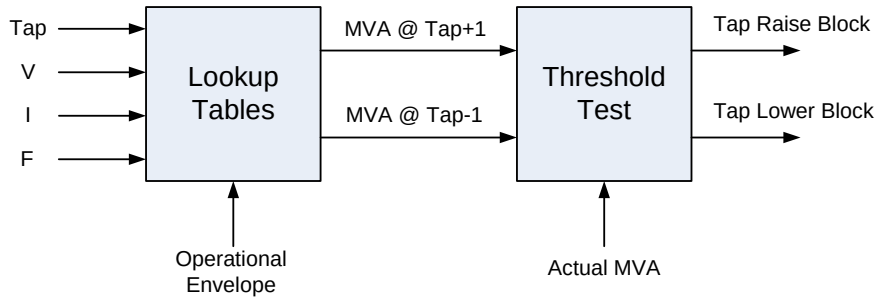

Figure 3-5 Typical QB local control system [33]

The protection arrangements for a QB are similar to those used for a power transformer. Four main functions are usually specified [32]:

- Overall current differential protection.
- LV earth fault protection.
- Temperature winding alarm and protection.
- Buccholz protection.

3.3.3 Setting of distance protection for transmission lines with QBs

There is no specific National Grid policy with regards to this matter. However, the policy statement indicates that zone 2 should provide remote busbar coverage taking into account maximum QB impedance at maximum boost or buck operation. Zone 3 should be set to provide coverage of the longest line connected to the remote busbar. However, these may result in excessive overreach should the QB be bypassed. Therefore the policy recommends 150% reach for zone 2 and relies on zone 3 to provide backup should 150% reach setting fall short of covering the remote busbar.

Although this recommendation may be suitable for the existing control regime, it remains static and does not take into account plans to implement coordinated QB control. This not only introduces more variability in the expected QB modes but also makes coordination of distance zone between adjacent circuits more challenging while risking lower levels of performance as indicated by the recommended settings. The coordinated control strategy is discussed in the following section.

3.3.4 Coordinated control of QBs

Operating a QB or a collection of QBs dynamically provides operational advantages especially in maximising post-fault circuit capacity [34]. However, the impact of a QB is not merely localised. Steady state studies on the PSTs in European transmission networks have shown the effect a single QB has on the adjacent circuits [35]. This then becomes an optimisation problem which should take into account the wider effects on the system. Nevertheless, providing a coordinated (or centralised) means of operating QBs is advantageous given that the coordination issues are resolved. Furthermore, as part of delivering this coordinated control approach, some QBs are installed in substations with the ability to switch between two circuits as dictated by the operational requirements [17]. Moving towards a coordinated QB control strategy means that the operating mode and tap position of a specific QB is not known beforehand and highly variable. The impact this may have on distance protection will be examined in the following section.

3.4 The evaluation of the impact of QBs on distance protection performance

This section presents the results of the evaluation of the distance protection performance for circuits containing QBs. At the time of writing this thesis, these were the only related comprehensive studies available where preliminary results were published in [17]. Work published by Dash et al [36] partially examined a similar problem. It was limited to power electronic based phase shifting transformers. Moreover, the results presented were only for resistive single phase faults at a single fault position.

3.4.1 Evaluation methodology

Simulations were conducted on the RTDS platform. This will facilitate the testing of the developed adaptive protection solution using a hardware in the loop approach as shown in the remainder of the thesis. The primary system data were obtained from the National Grid seven year statement for winter 2010/11 [37].

Figure 3-6 shows a single line diagram of the modelled network. The network section contains two QBs (QB1 at HIGM substation and QB2 at STAY substation). This enabled testing the impact of simultaneous QB operation on distance protection. Furthermore, the size of the network was chosen to allow the application and evaluation of zone 3 distance protection. The model data is summarised in Appendix A.

The relaying point is denoted by 21 in Figure 3-6. The distance protection model used was that offered by the RTDS standard components library, which is a multifunctional distance relay block [38]. This offers the use of Mho or quadrilateral characteristic. The former was used as it is the prevailing characteristic in the UK transmission network. Furthermore, the settings used are those specified in the National Grid policy and are summarised in Appendix A. No communications-based schemes were considered in this study. Furthermore, DAR functionality was disabled as the study is interested in quantifying the impact of the QB on the distance protection reach in isolation of circuit restoration post transient faults, so all faults applied were of a

permanent nature. Different fault types were placed on the line between HIGM and RATS substations (i.e. downstream of QB1). The faults were positioned at 0%, 30% 50%, 70% and 100% of the concerned line length. The impedance measured by the distance relay was observed for a range of QB modes and tap positions.

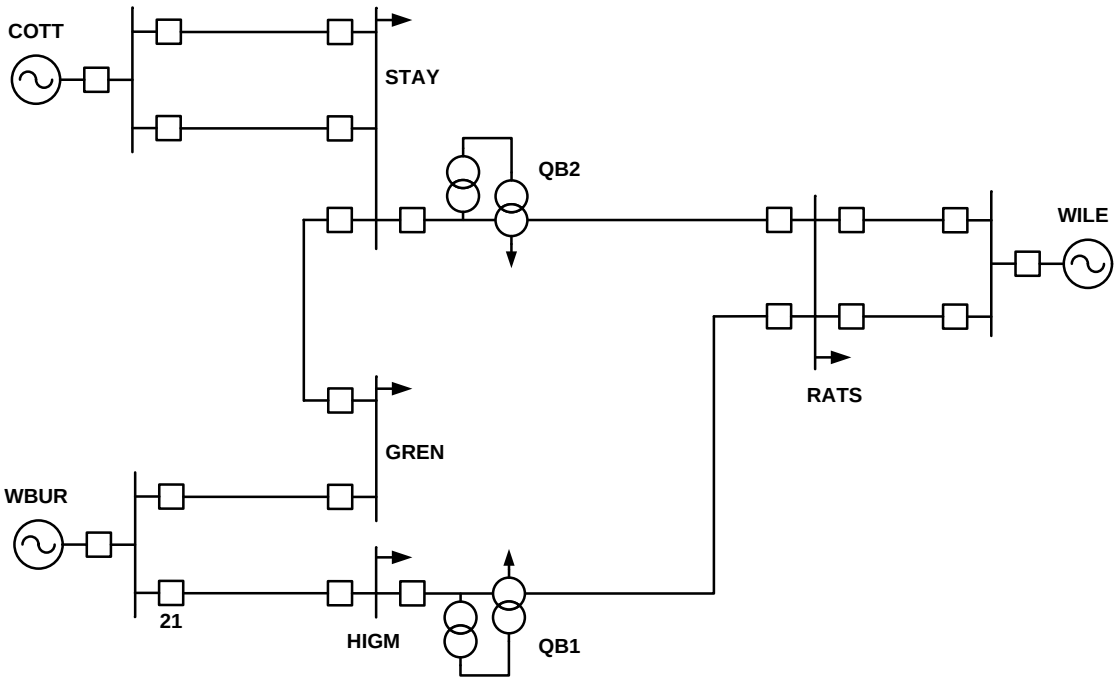

Figure 3-6 Modelled primary system single line diagram showing QB positions

3.4.2 QB model

The QB was modelled by connecting a phase shifting transformer (PST) windings in an extended delta configuration as shown in Figure 3-7 [32] to provide the quadrature voltage injection for QB operation. The PST model in the RTDS only provided eight tapping positions. This does not affect the possible maximum and minimum impact of tap positions, only the resolution of the results would be limited. The rating of the QB used was 2750MVA with an impedance of 15% (rating base) [37].

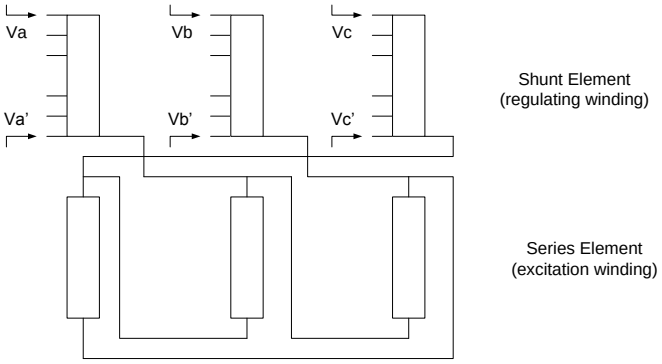

Figure 3-7 QB in extended delta winding connection

Figure 3-8 shows the QB introduced phase shift vs. the QB tap position in both boost and buck modes. The phase shift angle is calculated as the additional voltage angle difference introduced by the QB between busbars HIGM and RATS. The relationship between the line power and QB tap position is shown in Figure 3-9. This is only indicative as the power flow depends on the circuit configuration. The power flow as a result of the simultaneous operation of both QBs as well as other related operational issues is out with the scope of this chapter.

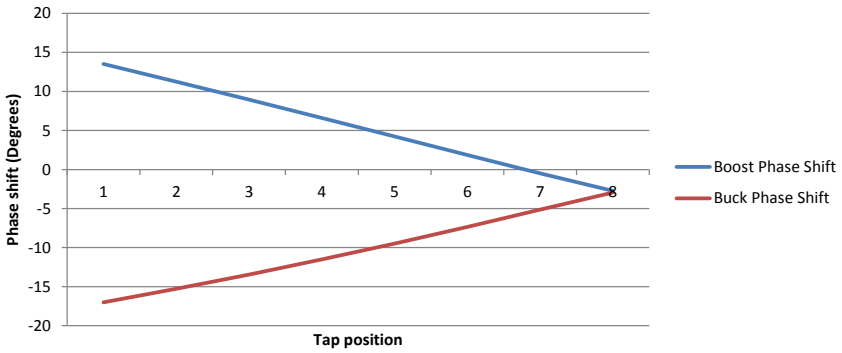

Figure 3-8 QB introduced phase shift vs. tap position

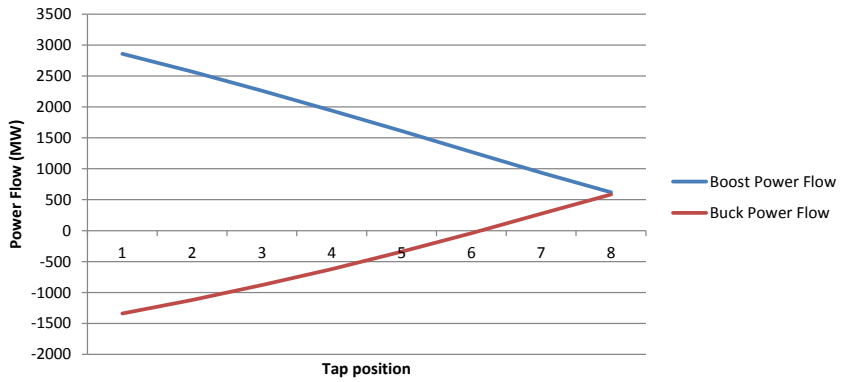

Figure 3-9 Circuit power flow vs. QB tap position

3.4.3 Results of the distance protection reach evaluation

The results of the simulations are summarised in the following tables. Since only asymmetrical faults result in errors in the impedance reach [17], single phase (A phase to ground, AG) and phase to phase (A phase to B phase, AB) faults are presented. Table 3-1 to Table 3-5 present the impedance measured by the relay for the single phase (Z_{AG}) and phase to phase faults (Z_{AB}) located at 0% to 100% of the HIGM-RATS circuit. The range of tap position presented is taps 1, 3 and 5 with tap 1 being the most extreme in boosting or bucking effect. All measured impedances fall within the appropriate protection zone for taps higher than 5. A measured impedance error is also presented and is calculated relative to the fault impedance when the QB is bypassed.

Results for resistive faults are also presented in Table 3-6 for AB faults at 50% line length. It should be emphasised that the detection of resistive faults and solutions related to this problem are out with the scope of this thesis.

Finally, Table 3-7 presents the measured impedance for simultaneous QB operation. A middle tap position was chosen for QB1 while tap 1 was selected for QB2 to maximise the potential impact on the measured impedance. The results in Table 3-7 are similar to those in Table 3-3 for individual QB operation.

Table 3-1 Measured impedance and impedance error for faults at 0% line length

Fault position	Fault type	QB mode	Tap position	$Z_{AG, AB}$				$Z_{AG, AB}$ error			
				R (Ω)	X (Ω)	|Z|(Ω)	<Z (°)	R (Ω)	X (Ω)	|Z|(Ω)	<Z (°)
0%	AG	Bypass	-	0.14	1.23	1.24	83.69	0.00	0.00	0.00	0.00
		Boost	1	1.13	0.92	1.45	39.00	0.99	-0.32	1.04	-17.58
			3	0.91	1.01	1.36	47.95	0.78	-0.22	0.81	-15.85
			5	0.65	1.10	1.28	59.61	0.51	-0.13	0.53	-14.33
		Buck	1	-1.23	1.47	1.92	129.92	-1.37	0.24	1.39	170.04
			3	-0.81	1.47	1.68	118.74	-0.94	0.24	0.97	165.71
			5	-0.39	1.39	1.44	105.79	-0.53	0.16	0.55	163.17
	AB	Bypass	-	0.16	1.22	1.23	82.39	0.00	0.00	0.00	0.00
		Boost	1	1.60	1.08	1.93	34.02	1.44	-0.14	1.44	-5.56
			3	1.24	1.12	1.67	42.09	1.08	-0.10	1.08	-5.30
			5	0.85	1.17	1.45	54.00	0.69	-0.05	0.69	-4.16
		Buck	1	-1.57	1.58	2.23	134.82	-1.73	0.36	1.77	168.26
			3	-0.99	1.50	1.80	123.40	-1.15	0.28	1.19	166.34
			5	-0.47	1.40	1.48	108.63	-0.64	0.18	0.66	164.17

Table 3-2 Measured impedance and impedance error for faults at 30% line length

Fault position	Fault type	QB mode	Tap position	$Z_{AG, AB}$				$Z_{AG, AB}$ error			
				R (Ω)	X (Ω)	|Z|(Ω)	<Z (°)	R (Ω)	X (Ω)	|Z|(Ω)	<Z (°)
30%	AG	Bypass	-	0.28	2.84	2.85	84.47	0.00	0.00	0.00	0.00
		Boost	1	1.66	1.87	2.50	48.40	1.39	-0.97	1.69	-35.01
			3	1.41	2.13	2.55	56.50	1.14	-0.71	1.34	-32.03
			5	1.06	2.42	2.64	66.35	0.79	-0.42	0.89	-28.15
		Buck	1	-2.07	3.17	3.79	123.14	-2.35	0.33	2.37	171.99
			3	-1.40	3.23	3.52	113.43	-1.68	0.39	1.72	166.89
			5	-0.69	3.17	3.24	102.33	-0.97	0.33	1.02	161.18
	AB	Bypass	-	0.32	2.80	2.82	83.52	0.00	0.00	0.00	0.00
		Boost	1	2.06	1.94	2.83	43.28	1.74	-0.86	1.94	-26.27
			3	1.69	2.16	2.74	51.96	1.37	-0.64	1.51	-25.01
			5	1.24	2.41	2.71	62.77	0.92	-0.39	1.00	-22.93
		Buck	1	-2.63	3.57	4.43	126.38	-2.95	0.77	3.05	165.36
			3	-1.67	3.48	3.86	115.64	-1.99	0.68	2.10	161.12
			5	-0.78	3.28	3.37	103.36	-1.10	0.48	1.20	156.37

Table 3-3 Measured impedance and impedance error for faults at 50% line length

Fault position	Fault type	QB mode	Tap position	$Z_{AG, AB}$				$Z_{AG, AB}$ error			
				R (Ω)	X (Ω)	|Z|(Ω)	<Z (°)	R (Ω)	X (Ω)	|Z|(Ω)	<Z (°)
50%	AG	Bypass	-	0.37	3.91	3.93	84.57	0.00	0.00	0.00	0.00
		Boost	1	1.97	2.46	3.15	51.31	1.60	-1.45	2.16	-42.22
			3	1.73	2.84	3.33	58.65	1.36	-1.07	1.73	-38.24
			5	1.33	3.28	3.54	67.93	0.96	-0.63	1.15	-33.33
		Buck	1	-2.57	4.24	4.96	121.22	-2.94	0.33	2.96	173.60
			3	-1.78	4.38	4.73	112.12	-2.15	0.47	2.20	167.68
			5	-0.89	4.34	4.43	101.56	-1.26	0.43	1.33	161.16
	AB	Bypass	-	0.42	3.86	3.88	83.79	0.00	0.00	0.00	0.00
		Boost	1	2.33	2.48	3.40	46.79	1.91	-1.38	2.36	-35.85
			3	1.98	2.82	3.45	54.93	1.56	-1.04	1.87	-33.69
			5	1.51	3.22	3.56	64.88	1.09	-0.64	1.26	-30.42
		Buck	1	-3.29	4.79	5.81	124.48	-3.71	0.93	3.82	165.93
			3	-2.11	4.76	5.21	113.91	-2.53	0.90	2.69	160.42
			5	-0.96	4.52	4.62	102.03	-1.38	0.66	1.53	154.49

Table 3-4 Measured impedance and impedance error for faults at 70% line length

Fault position	Fault type	QB mode	Tap position	$Z_{AG, AB}$				$Z_{AG, AB}$ error			
				R (Ω)	X (Ω)	|Z|(Ω)	<Z (°)	R (Ω)	X (Ω)	|Z|(Ω)	<Z (°)
70%	AG	Bypass	-	0.47	4.97	4.99	84.55	0.00	0.00	0.00	0.00
		Boost	1	2.26	3.02	3.77	53.19	1.79	-1.95	2.64	-47.51
			3	2.03	3.52	4.06	60.03	1.56	-1.45	2.13	-42.98
			5	1.62	4.11	4.42	68.49	1.15	-0.86	1.43	-36.89
		Buck	1	-3.04	5.27	6.08	119.98	-3.51	0.30	3.53	175.12
			3	-2.14	5.50	5.90	111.26	-2.61	0.53	2.67	168.54
			5	-1.06	5.50	5.60	100.91	-1.53	0.53	1.62	160.94
	AB	Bypass	-	0.55	4.91	4.94	83.62	0.00	0.00	0.00	0.00
		Boost	1	2.58	3.00	3.96	49.30	2.03	-1.91	2.79	-43.24
			3	2.26	3.45	4.12	56.77	1.71	-1.46	2.25	-40.47
			5	1.77	4.01	4.38	66.18	1.22	-0.90	1.52	-36.39
		Buck	1	-3.91	5.95	7.12	123.31	-4.46	1.04	4.58	166.87
			3	-2.54	6.00	6.52	112.94	-3.09	1.09	3.28	160.56
			5	-1.15	5.76	5.87	101.29	-1.70	0.85	1.90	153.42

Table 3-5 Measured impedance and impedance error for faults at 100% line length

Fault position	Fault type	QB mode	Tap position	$Z_{AG, AB}$				$Z_{AG, AB}$ error			
				R (Ω)	X (Ω)	|Z|(Ω)	<Z (°)	R (Ω)	X (Ω)	|Z|(Ω)	<Z (°)
100%	AG	Bypass	-	0.68	6.57	6.61	84.09	0.00	0.00	0.00	0.00
		Boost	1	2.68	3.79	4.64	54.73	2.00	-2.78	3.42	-54.27
			3	2.49	4.48	5.13	60.93	1.81	-2.09	2.76	-49.11
			5	2.06	5.31	5.70	68.80	1.38	-1.26	1.87	-42.40
		Buck	1	-3.77	6.75	7.73	119.18	-4.45	0.18	4.45	177.68
			3	-2.69	7.17	7.66	110.56	-3.37	0.60	3.42	169.90
			5	-1.33	7.28	7.40	100.35	-2.01	0.71	2.13	160.55
	AB	Bypass	-	0.76	6.49	6.53	83.29	0.00	0.00	0.00	0.00
		Boost	1	2.92	3.70	4.71	51.72	2.16	-2.79	3.53	-52.29
			3	2.66	4.35	5.10	58.55	1.90	-2.14	2.86	-48.44
			5	2.18	5.16	5.60	67.10	1.42	-1.33	1.94	-43.19
		Buck	1	-4.82	7.51	8.92	122.69	-5.58	1.02	5.68	169.65
			3	-3.19	7.79	8.42	112.27	-3.95	1.30	4.16	161.80
			5	-1.42	7.60	7.73	100.58	-2.18	1.11	2.45	153.05

Table 3-6 Measured impedance for resistive faults at 50% line length

Fault position	Fault resistance	Fault type	QB mode	Tap position	$Z_{AG, AB}$			
					R (Ω)	X (Ω)	|Z|(Ω)	<Z (°)
50%	5Ω	AG	Bypass	-	2.33	3.91	4.55	59.21
			Boost	1	2.89	1.92	3.47	33.60
				3	2.88	2.29	3.68	38.49
				5	2.8	2.82	3.97	45.20
			Buck	1	-0.98	6.1	6.18	99.13
				3	0.22	5.83	5.83	87.84
				5	1.31	5.19	5.35	75.83
		AB	Bypass	-	1.95	3.82	4.29	62.96
			Boost	1	3	2.02	3.62	33.95
				3	2.84	2.35	3.69	39.61
				5	2.61	2.82	3.84	47.21
			Buck	1	-1.97	6.49	6.78	106.89
				3	-0.43	5.98	6.00	94.11
				5	0.82	5.17	5.23	80.99
	10Ω	AG	Bypass	-	4.21	3.85	5.70	42.44
			Boost	1	3.72	1.55	4.03	22.62
				3	3.92	1.9	4.36	25.86
				5	4.1	2.45	4.78	30.86
			Buck	1	0.72	8.45	8.48	85.13
				3	2.48	7.48	7.88	71.66
				5	3.67	6	7.03	58.55
		AB	Bypass	-	3.41	3.72	5.05	47.49
			Boost	1	3.63	1.67	4.00	24.71
				3	3.63	1.98	4.13	28.61
				5	3.63	2.47	4.39	34.23
			Buck	1	-0.58	8.52	8.54	93.89
				3	1.43	7.32	7.46	78.95
				5	2.71	5.77	6.37	64.84

Table 3-7 Measured impedance for phase to phase fault at 50% line length for simultaneous QB operation

Fault position	Faul type	QB status				Z_{AB}			
		QB1 mode	QB1 tap	QB2 mode	QB2 tap	R (Ω)	X (Ω)	$\|Z_{AB}\|$(Ω)	$<Z_{AB}$ (°)
50%	AB	Bypass	-	Boost	1	0.43	3.89	3.91	83.69
		Bypass	-	Buck	1	0.43	3.90	3.92	83.71
		Boost	3	Boost	1	2.15	2.95	3.65	53.91
		Boost	3	Buck	1	1.82	2.83	3.36	57.25
		Buck	3	Boost	1	-1.99	4.57	4.98	113.53
		Buck	3	Buck	1	-2.16	5.10	5.54	112.95

The measurement impedance results have been illustrated in MHO diagrams to clearly present the reach issues influenced by QB operation. Only the worst case scenario faults in terms of reach error are shown (AB faults). In Figure 3-10 shows the fault impedance at the aforementioned locations when the QB is bypassed.

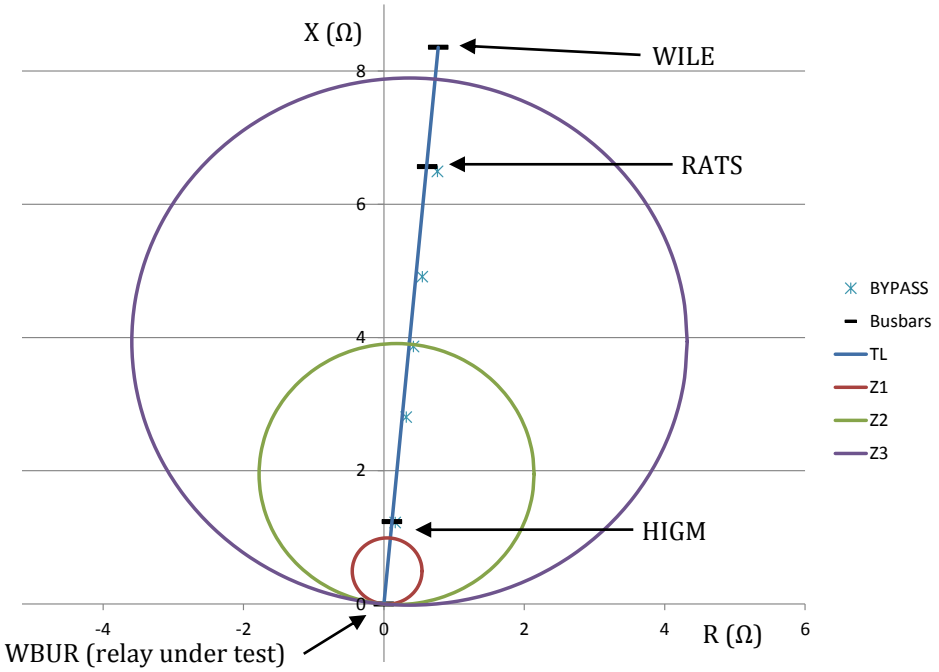

Figure 3-10 Fault impedance when QB is in Bypass mode

Figure 3-11 shows the measured fault impedance when the QB is in boosting mode. Each set of impedance points relating to a tap position are grouped for clarity. In this case the maximum error in measured impedance occurs for faults at 100% of the line length when the QB is at maximum tap (tap 1). All faults occur within the reach of zone 3.

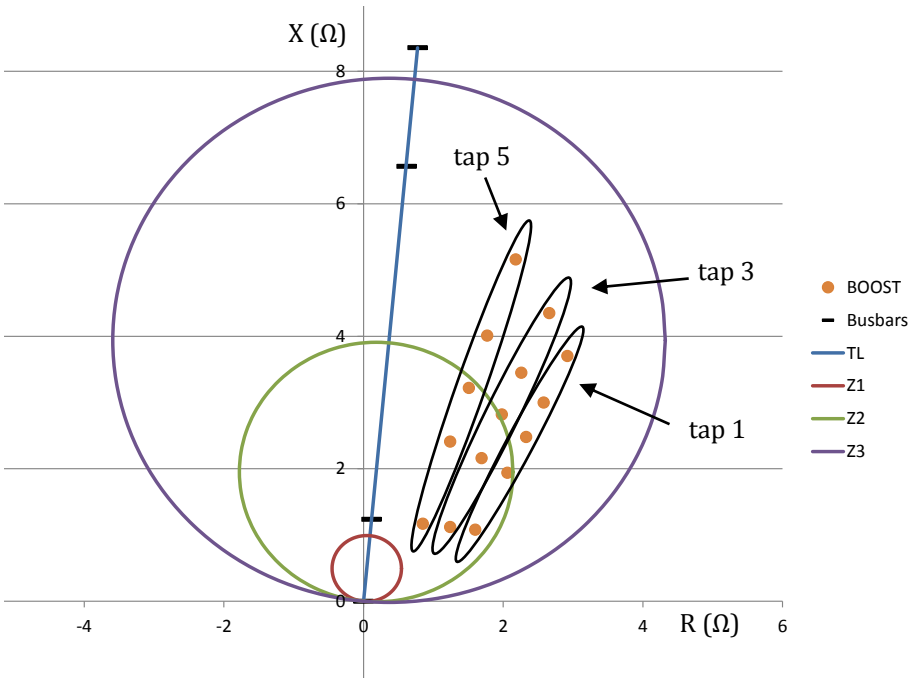

Figure 3-11 Fault impedance when QB is in Boost mode

Finally, the measured fault impedance during QB buck mode is illustrated in Figure 3-12. This shows that a greater error in the impedance measurement is introduced. The maximum reach error also occurs for faults at 100% line length and tap position 1. It can also be seen that some of the measured impedances are located out with zone 3.

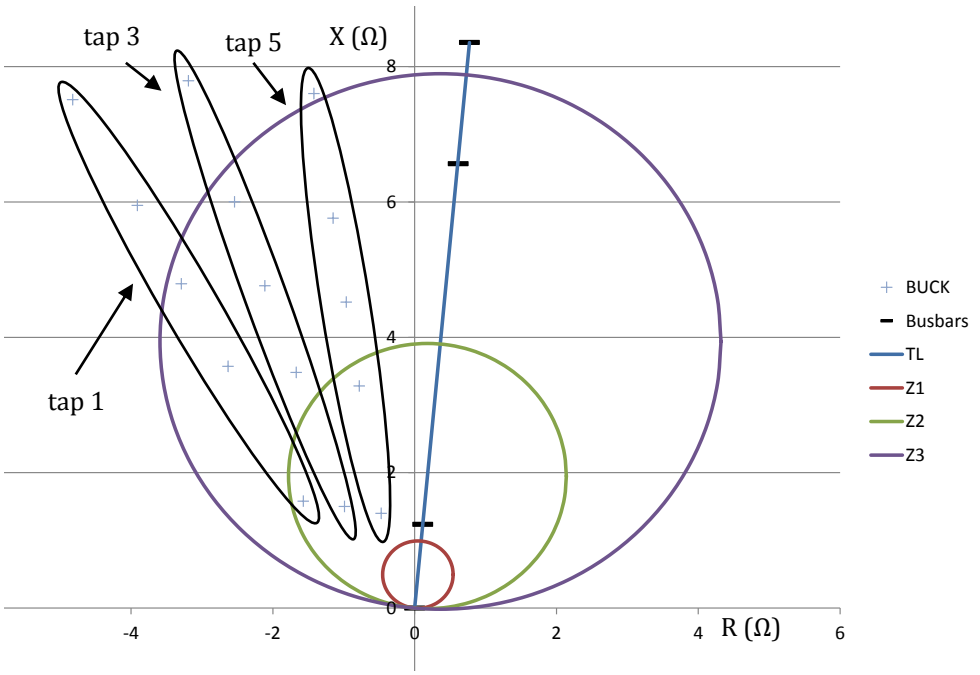

Figure 3-12 Fault impedance when QB is in buck mode

3.4.4 Discussion of reach impact due to QB operation

The results show that operating a QB in bucking mode always results in greater reach error compared to boosting mode for corresponding fault types and positions. For the range of faults applied in this study, the maximum reach error magnitude is 5.68Ω for maximum tap position. The corresponding error magnitude for boosting mode is 3.53Ω. The relationship between reach error and QB status (mode and tap position) is not strictly linear due to the offsets introduced by the inherent QB impedance. This is estimated in the following section.

The results also show that operating QBs simultaneously do not have an additional effect on the reach of an individual distance protection relay. However, for a coordinated QB control strategy it is important to consider the following operating conditions that were not envisaged by the system operator:

- Continuous change of QB status under coordinated control strategy means that settings calculated for the worst case scenario are not optimal. Also, setting for worst case scenarios may result in undesirable over reach when the QB is bypassed.

- QB switching between multiple circuits is also possible. This will have impact protection relays that were not previously affected by the presence of a QB in the protected circuit.

The impact of QB on distance protection reach is limited to back up zones 2 and 3. Zone 1 mal operation is mitigated by the relative placement of the protection relay under study to the QB. The degradation of performance of back up protection is an important problem that must be taken into consideration when assessing the reliability of the protection schemes in place. Not only because the performance specification of these back up zones are violated, but also to the greater important of ensuring protection reliability during flexible power system operating conditions.

3.4.5 A relation for measured impedance error vs. QB mode

In this section a measure for estimating the measured impedance error based on the QB mode will be established. In the following chapters, the impedance error magnitude will be incorporated in the development of an adaptive distance protection solution that takes into account this introduced error.

The impact of QB operation on the introduced error is not entirely linear as observed from the results so far. The relation can be derived either empirically or by calculating the impedance from the power system quantities. Either way, both approaches will require a means of modifying the relation based on the primary system considered. This is mainly to take into account the effect of different QB impedances. If a direct derivation is pursued, then the primary system model must be resolved in to its equivalent sequence network circuits. This must also be achieved for the QB transformer. Information on modelling the QB sequence circuits can be found in [39]. One of the difficulties in using these QB equivalent circuits is that they do not directly apply to the extended delta QB model used in the simulations reported in this chapter. This is because the extended delta model does not consist of shunt and series elements, but

rather field and regulating windings to which the sequence network equivalents found in [39] do not apply.

The alternative approach based on an empirical evaluation of the relation describing the impact on impedance will provide an estimate based on the specific simulation results reported in this chapter. An estimation in this case is valid since the reach of a distance protection zone is usually specified with a tolerance of +/-5% based on IEC 60255 [40]. To achieve this, it is proposed that the derived relation reflects the different factors that impact the reach error, these are:

- The position of the fault along the protected transmission line.
- Inherent impedance offset introduced by the QB.
- The QB tap position and mode of operation.

The reach error can manifest itself on either side of the protected line in the R-X impedance plane of the Mho distance protection characteristic according to the QB mode (i.e. boost or buck). Thus, the reach error is a complex quantity. However, it is deemed sufficient to only calculate the magnitude of the reach error as the position of the impedance point relative to the protected circuit can be determined based on knowledge of the QB mode.

The impedance reach error magnitude $|\Delta Z|$ is defined as the distance between the impedance locus without the effect of QB to that when the QB is connected to the circuit. This is illustrated in Figure 3-13.

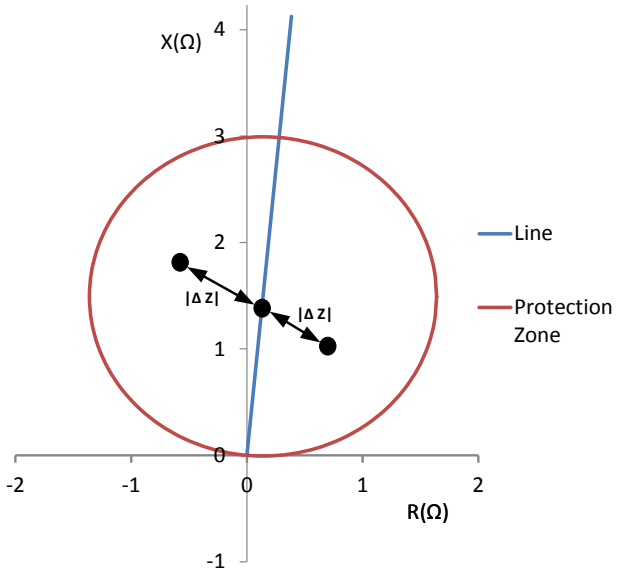

Figure 3-13 Mho characteristic showing how the reach error magnitude is measured

When taking these different factors into account and the definition of the reach error magnitude, then $|\Delta Z|$ can be estimated by (1):

$$|\Delta Z| = (|Z_{min}| + |Z_{offset}| \times l) \times \alpha \qquad (1)$$

Where, $|Z_{min}|$ is the magnitude of the minimum error impedance introduced by the QB (at fault position 0% and tap position 5), $|Z_{offset}|$ is the additional impedance offset introduced for each percentage point of line length l and α is a multiplier that depends on the tap position and QB mode. With each tap position change, the impedance locus 'jumps' to a different position which is reflected by a step change of reach error.

In order to devise values for the parameters in (1), the results in Table 3-1 to Table 3-5 and corresponding Figure 3-10 to Figure 3-12 must be examined. Note that all values are based on the worst case scenario faults (i.e. line to line faults). $|Z_{min}|$ can be determined readily by measuring the distance between the normal fault impedance and the shifted fault impedance at a fault position of 0% and tap position of 5. Therefore the values for $|Z_{min}|$ can be found in Table 3-1 under $|Z_{AB}|$ error and are 0.69 Ω and 0.66Ω for boost and buck modes respectively.

To determine the value of $|Z_{offset}|$, first of all the average of the difference between impedance error magnitudes in consecutive tap positions is calculated. Secondly, this average is taken with the corresponding average for a different fault position and the difference between these two values is calculated. Finally, the calculated difference is divided by the percentage length difference between the compared fault positions. To illustrate this process, consider Figure 3-14 in conjunction with the presented simulation results. The average of calculated $|\Delta Z_1|$ and $|\Delta Z_2|$ is determined as $|\Delta Z_A|$. This process is repeated to obtain the average $|\Delta Z_B|$ for the calculated values of $|\Delta Z_3|$ and $|\Delta Z_4|$. Note that $|\Delta Z_1|$ to $|\Delta Z_4|$ should not to be confused with the reach error $|\Delta Z|$. These are the difference between two reach error values for two consecutive tap positions. Finally, the difference between the averages $|\Delta Z_A|$ and $|\Delta Z_B|$ is then divided by ΔL to obtain a per length percentage value of the offset. $|Z_{offset}|$ essentially increases with each increment in fault position along the protected line.

Based on the simulation results, the calculated values for $|Z_{offset}|$ vary slightly across the range of simulated fault positions. The values chosen were for faults at 50% for buck and 70% for boost. These values represent the closest impedance points to the boundary of zone 2. As such, these can be used as a threshold to determine when an extension in the zone reach is necessary to compensate for the under reach caused by the QB.

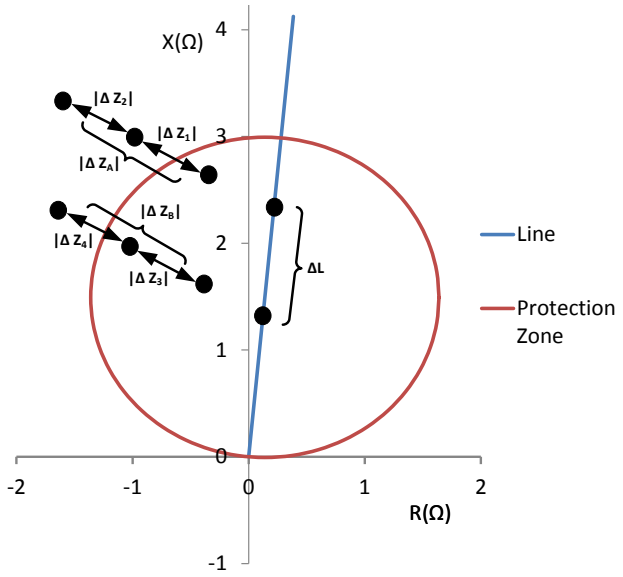

Figure 3-14 Mho diagram illustrating process of determining $|Z_{offset}|$

In addition to the offsets $|Z_{min}|$ and $|Z_{offset}|$, α is used to reflect the 'jumps' in impedance error at different QB tap positions. Since the impedance positions between different taps are not equidistant, the values for α are obtained by assuming an initial value then fine tuning it while comparing the resulting $|\Delta Z|$ with the values of "$|Z_{AB}|$ error" in the previous results tables. The values for $|Z_{min}|$, $|Z_{offset}|$ α and are summarised in Table 3-8.

Table 3-8 Variables used for the estimation of impedance error magnitude

	Boost	Buck
$\|Z_{min}\|$	0.69Ω	0.66Ω
$\|Z_{offset}\|$	0.004Ω/length %	0.011Ω/length %
α (tap5)	1.8	1.5
α (tap3)	2.2	2
α (tap1)	3	3

3.5 Sensitivity and stability evaluation of loss of mains protection

Loss of mains (LOM) protection is used to disconnect distributed generation (DG) should it become islanded from the main grid [12]. Islanded operation of DER is currently prohibited by policy as indicated by engineering recommendations ER G59/2 [41] and IEEE standard IEEE 1547 [42] due to the following reasons:

- Safety hazard to personnel due the potential energisation of a network section that would otherwise be offline when isolated from the grid.
- The possibility of out of phase reclosure between an energised islanded network and the main grid.
- Inability of the DER to maintain power quality limits.

Loss of mains protection can usually be easily detected by voltage and frequency protection due to the excursions these quantities may experience when local generation (DER) and load are mismatched. However, for situations when the DER is able to reliably meet the deficit in generation or when the load and local generation are mostly matched, the detection of LOM becomes more difficult. Other methods are then used for this purpose, the most common of which are rate of change of frequency (ROCOF) and voltage vector shift (VS) [12].

Although effective in detecting LOM events, ROCOF and VS under certain operating conditions suffer from spurious tripping following remote disturbances whether caused by faults or rapid frequency excursions [43]. Spurious tripping violates fundamental stable performance criteria required by all protection schemes. Increasing the pick-up setting can provide immunity against the causes of such spurious trips, but at the cost of LOM detection sensitivity. Another dimension to the problem is introduced by the different DG technologies that are becoming commonplace. To this end, this section reports on the investigation of the impact of different generating conditions coupled with different LOM or remote disturbance scenarios on the performance of LOM protection.

3.5.1 Methodology

At the time of conducting these tests, they were the first of their kind in terms of providing a comprehensive study covering a wide range of scenarios, generator technologies and LOM protection relays. This work was then published in [43]. Two main performance criteria were evaluated. These are the sensitivity of LOM protection to true LOM events and the stability of LOM protection against system disturbances. Furthermore, four DG technologies were considered:

- Synchronous machine (30MVA at 33kV and 3MVA at 11kV).
- DFIG (30MVA at 33kV and 3MVA at 11kV).
- Induction machine (0.86MVA at 11kV).
- Inverter connected DC source (1.5MVA at 11kV).

The generator output is set initially at 90% of rated MVA prior to islanding which is initiated by opening of the point of common coupling (PCC). A number of different loading scenarios were considered to examine the extent of relay sensitivity to generation-load imbalance post LOM event. The active and reactive power consumption of the local load was varied to give a net import/export range across the PCC of (0%, 2.5%, 5% and 10%) of DG rated MVA. Active and reactive power imbalance are considered in isolation, such that imbalance in net active power import/export is associated with 0% imbalance in reactive power and vice-versa.

For stability testing, faults are applied at different locations in the network such that the retained voltage at the DER terminals is at 20%, 50% and 80% of nominal value which is then captured in COMTRADE format. It was necessary to modify the fault resistance in some of the scenarios to obtain these retained voltage levels. The faults applied were of single phase to ground, phase to phase and three phase type. To minimise the effect of generation-load imbalance on the stability tests, the net import/export of power across the PCC was set to 0% of the DG rated MVA. Furthermore, faults were applied for a maximum duration of 0.5s and 1s respectively for the 33kV and 11kV networks respectively. These are considered typical maximum fault clearance times for these voltage levels.

Commercial relays from three different manufacturers were used to assess the performance of the of the LOM algorithms – these are referred to as Relay 1, Relay 2 and Relay 3 due to commercial sensitivities. The obtained voltage waveforms from sensitivity and stability tests are injected into the relays to observe their response and tripping times were recorded. The boundary settings were determined for each test scenario. The testing procedure is depicted in Figure 3-15.

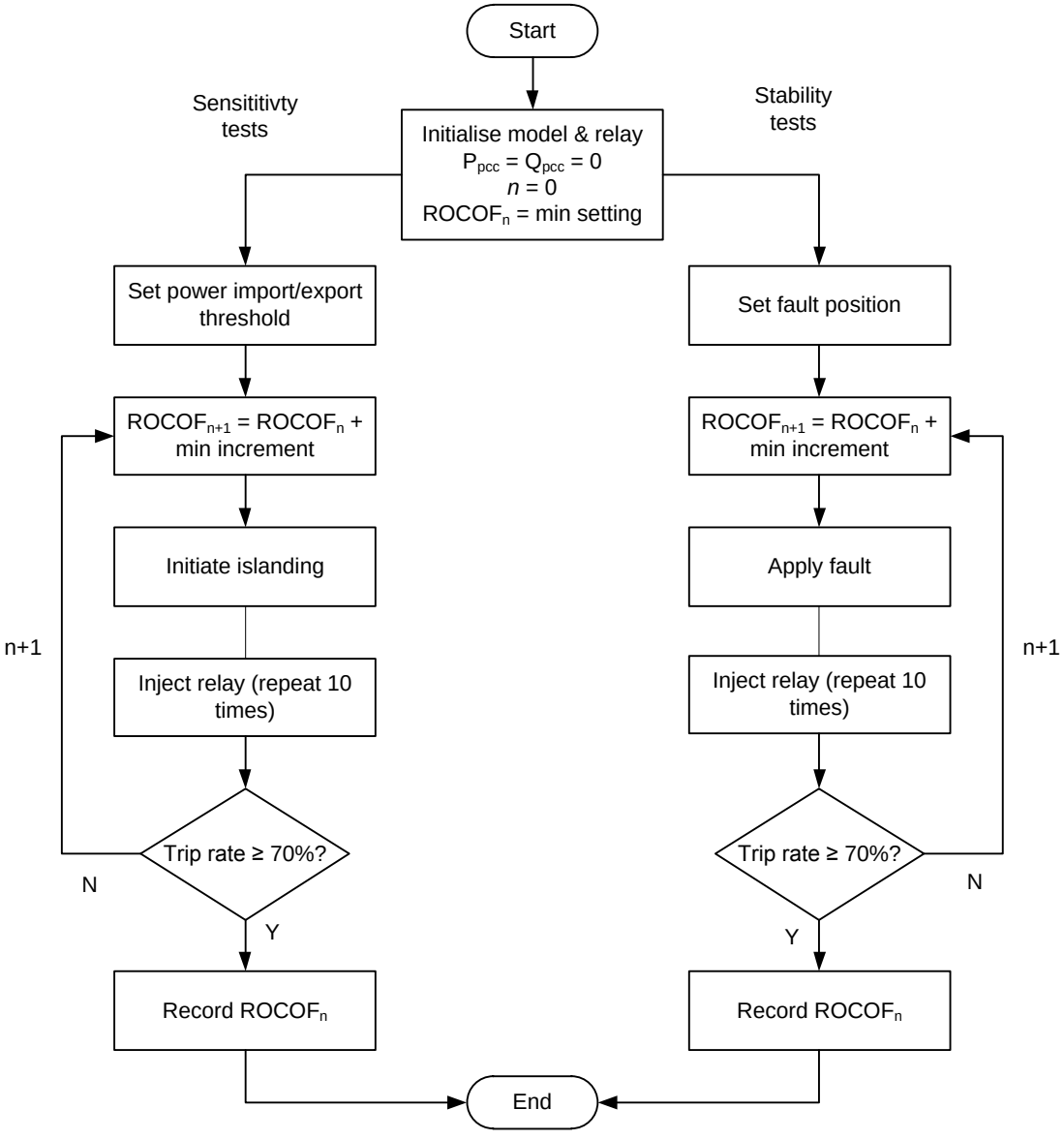

Figure 3-15 LOM sensitivity and stability testing procedure

3.5.2 Power system models

The 33kV network used is an equivalent reduced network from the Scottish Power distribution network and is shown in Figure 3-16 with fault locations indicated. The 11kV test network and data was obtained from CE Electric and is shown in Figure 3-17. Associated network and generator data can be found in [43].

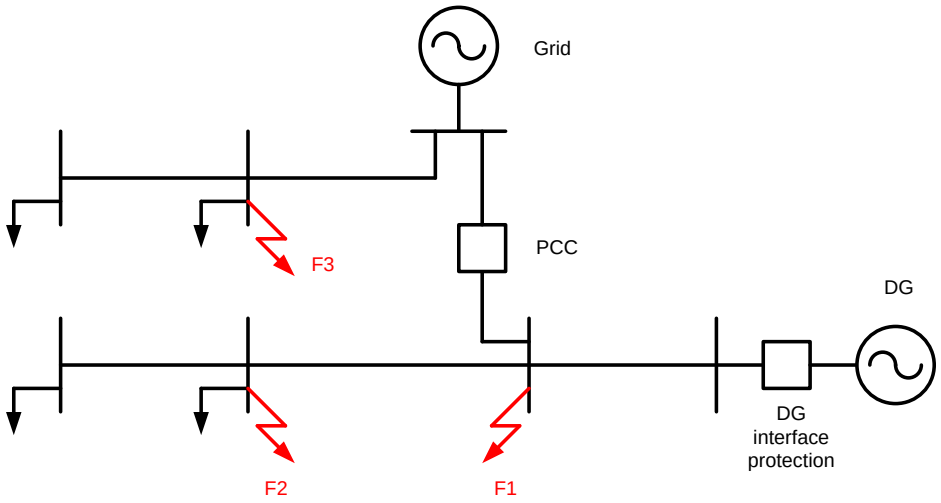

Figure 3-16 33kV test network

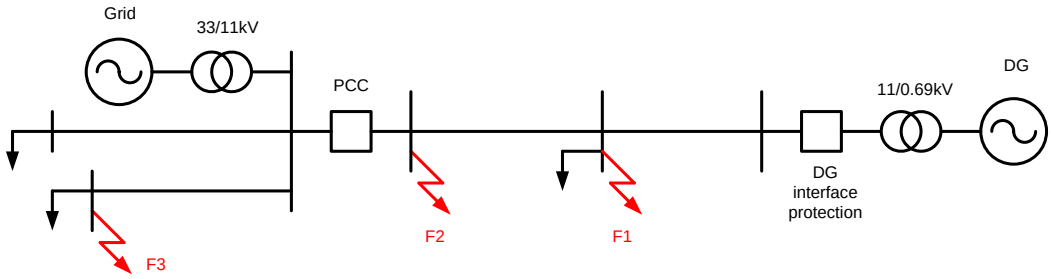

Figure 3-17 11kV Test network

Once the tests were completed, compromise settings were suggested for each DG size and technology. These compromise settings offer a balance between LOM protection sensitivity and stability. The full set of results can be found in [43]. But for the purposes of the discussion in this chapter two sets of results are emphasised in the following sections.

3.5.3 Compromise settings for DFIG based generation

Table 3-9 shows the response of relay 1 for a range of tests and settings for a 3MVA DFIG generator connected to the 11kV test network. In this case, the suggested best setting is 3Hz/s (highlighted in grey). Applying this setting can potentially desensitise the relay to true loss of mains events. So a compromise may be required at the expense of lower stability against remote disturbances. Such compromise settings may become obsolete with variable network conditions.

Table 3-9 Compromise relay 1 ROCOF settings for 3MVA DFIG generator connected to 11kV network

Setting	Sensitive to LOM with 5% active imbalance	Sensitive to LOM with 5% reactive imbalance	Stable for 20% retained voltage faults (ph-e, ph-ph, 3-ph)	Stable for 50% retained voltage faults (ph-e, ph-ph, 3-ph)	Stable for 80% retained voltage faults (ph-e, ph-ph, 3-ph)
0.5Hz/s, 0ms	Y	Y	Y,N,N	Y,N,Y	Y,Y,Y
0.5Hz/s, 120ms	Y	Y	Y,N,N	Y,N,Y	Y,Y,Y
0.5Hz/s, 240ms	N	N	Y,Y,Y	Y,Y,Y	Y,Y,Y
1.5Hz/s, 0ms	Y	Y	Y,N,N	Y,N,Y	Y,Y,Y
1.5Hz/s, 120ms	Y	Y	Y,Y,N	Y,N,Y	Y,Y,Y
1.5Hz/s, 240ms	N	N	Y,Y,Y	Y,Y,Y	Y,Y,Y
3Hz/s, 0ms	Y	Y	Y,Y,Y	Y,N,Y	Y,Y,Y
3Hz/s, 120ms	Y	Y	Y,Y,Y	Y,Y,Y	Y,Y,Y
3Hz/s, 240ms	N	N	Y,Y,Y	Y,Y,Y	Y,Y,Y

3.5.4 Performance discrepancies between different ROCOF algorithms

The next set of results is related to the sensitivity of Relays 1-3 for a 30MVA synchronous generator based DG connected to the 33kV test network. The boundary settings for these relay are shown Figure 3-18 to Figure 3-20 for different amounts of active and reactive power imbalance.

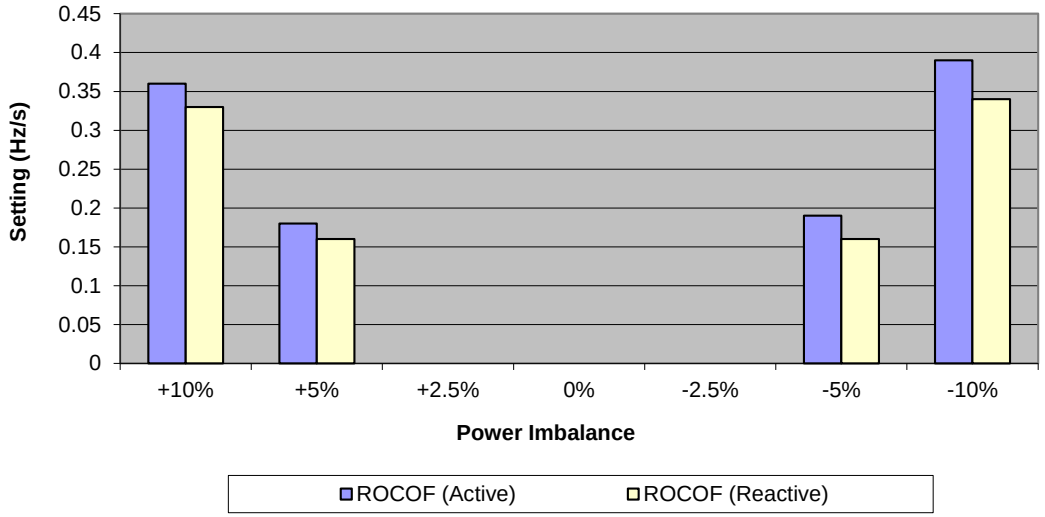

Figure 3-18 Maximum sensitivity settings for 30MVA synchronous DG connected to 33kV network – relay 1

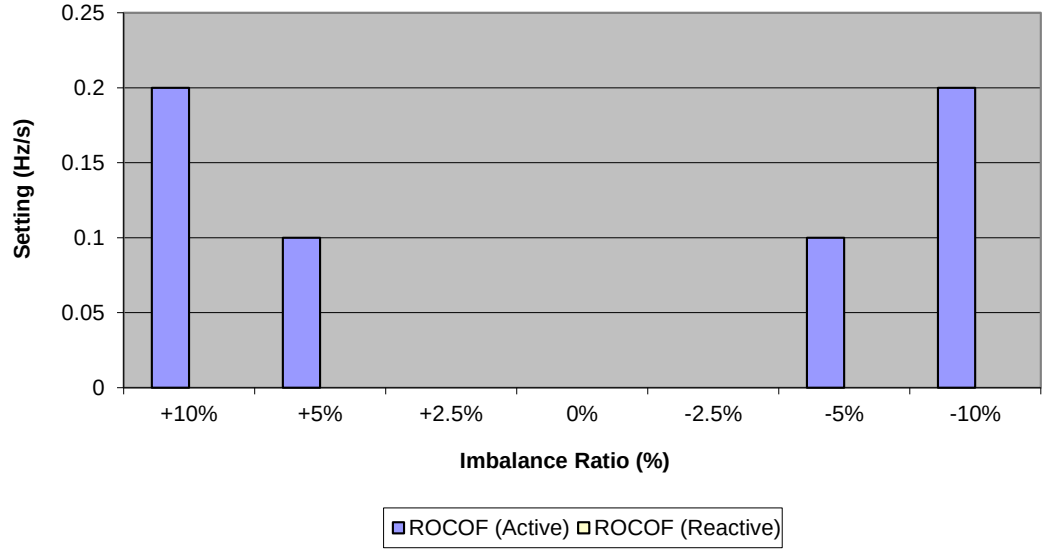

Figure 3-19 Maximum sensitivity settings for 30MVA synchronous DG connected to 33kV network - relay 2

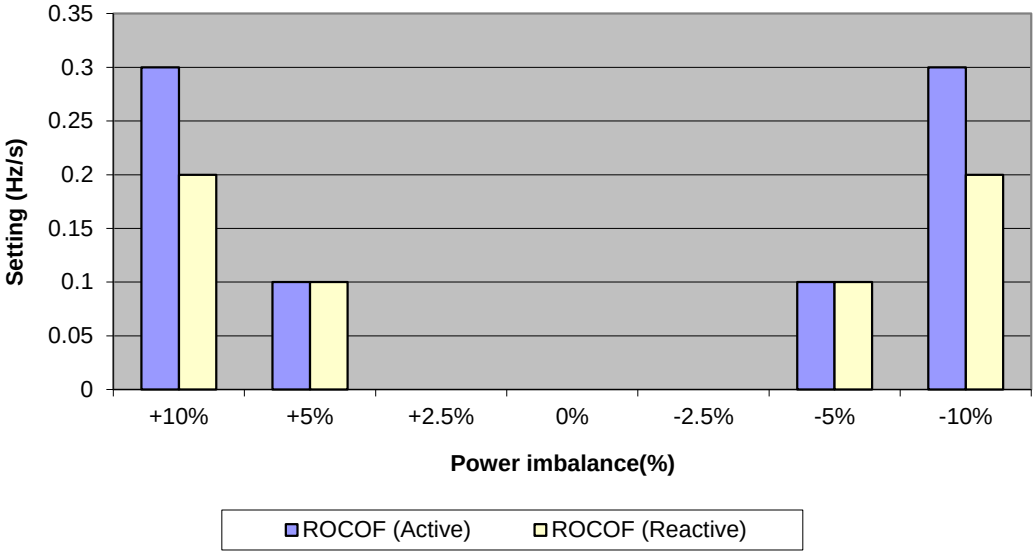

Figure 3-20 Maximum sensitivity settings for 30MVA synchronous DG connected to 33kV network - relay 3

The results show that the maximum settings for 10% active power import ranges between 0.2 and 0.39Hz/s. Relay 2 does not respond to reactive power imbalanced under these test conditions.

It is clear from these results that different manufacturer implementations of the same protection principle can result in varied performance. One of the main reasons that this can be attributed to is the implementation of frequency and rate of change of frequency measurement of the different relays. As such it is difficult to guarantee a consistent level of performance for ROCOF based LOM protection. This particular issue is discussed further in 3.6.3.

3.6 Robust vs. flexible protection scheme performance

The discussion in the previous section has drawn out a very important conclusion. That is for a protection scheme to always perform according to specified requirements under all primary system operational conditions, it is at least required that the protection settings match the primary system condition. Meeting these performance requirements under all possible operational conditions necessarily means that the protection scheme behaviour needs to exhibit a degree of robustness. Flexible primary system operation results in uncertainty in operating conditions, and robustness in behaviour can cope with the risk of poor performance associated with uncertainty. The challenge herein lies in achieving robust behaviour. To this end, it is necessary to understand robustness from the point of view of protection scheme and in light of flexible primary system operation.

3.6.1 Robust behaviour of protection systems

[44] outline an important relationship between the robustness a system can exhibit and the specialisation it can provide in terms of functionality. Robustness entails a predetermination of behaviour against a large range of perturbations which inherently results in the system performing in a sub-optimal manner. Protection schemes are mostly geared towards robust operation (this is different from gearing the protection towards dependable operation). To illustrate this concept, consider an overcurrent protection scheme. The primary system current $i(t)$ is monitored and a trip decision is based on the current in relation to the protection characteristic (IDMT, DT, etc.). As shown in Figure 3-21, the current trajectory $i_0(t) \rightarrow i_1(t)$ as a result of a fault condition leads to the correct tripping of the overcurrent relay. It can also be seen that both under healthy and faulty system conditions the system current $i(t)$ can vary based on loading, network configuration, fault impedance, etc. However, the protection remains robust against these variations. The main factor dictating the robustness in protection behaviour in this case is the protection setting which demarcates the healthy and faulty conditions.

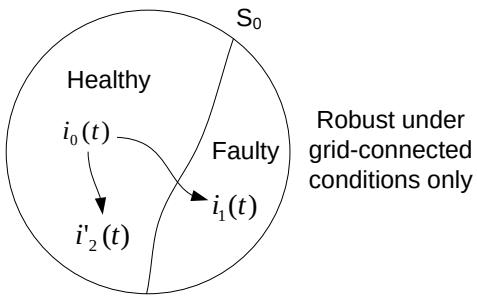

Figure 3-21 Primary current trajectory under normal operating conditions

If the network was operated in an islanded condition with inverter-interfaced DER, then the fault current $i'_2(t)$ would reduce significantly which impacts the sensitivity of the installed overcurrent protection. In this case, the generalised operation of the protection functions leads to unsatisfactory performance with an increased risk of failure to detect the fault as shown in Figure 3-21. The protection setting being inappropriate in this case (non-specialised) resulted in the failure to of protection operation due to its desensitisation.

This poses a further challenge to the one presented in the previous section. Not only does a protection scheme need to achieve robust behaviour but it also must ensure that existing protection settings are valid for increasingly variable primary system conditions.

3.6.2 The need for flexible power system protection

Flexible operation of the primary system, under specific conditions, requires the dynamic alteration of the scheme behaviour in order to maintain sought levels of performance. A means of making robust behaviour suited (or specialised) to different operating conditions is then required. This can be achieved through flexible operation of the protection system. To address the example given in the previous section, the setting is changed dynamically to reflect the different operational conditions as shown in Figure 3-22.

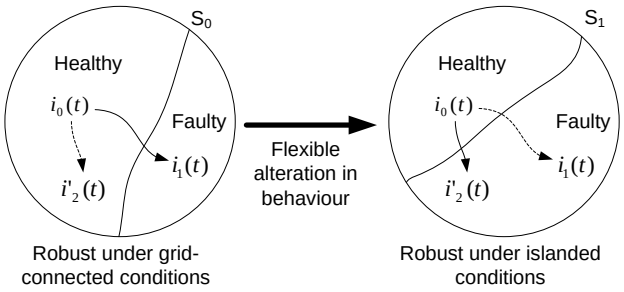

Figure 3-22 Flexible changes in protection setting and new system current trajectory

This illustrates that the robustness of the system can be altered to suit specific operating conditions. And this is achieved through flexibly changing the protection scheme behaviour by changing to the most appropriate setting for the given situation. The protection system therefore can be immune to the performance impact of different operational conditions on the basis that it exhibits flexibility in behaviour to support its inherent robustness. The topology of the system can be used as means of determining the need to change the robustness boundaries of the system. At this point in the discussion, the QB example discussed previously can be invoked. Energising a QB and tapping it at different positions can have a detrimental impact on distance protection reach and so the robustness of the Mho zones can no longer deliver satisfactory performance. To rectify this, a flexible Mho characteristic can be achieved by altering the zone reaches through settings to meet the conditions dictated by the QB. This shows that flexible alteration of protection settings can achieve robustness against a defined set of primary system conditions. As a direct conclusion, it can be said that it is necessary for some protection schemes to be flexible to maintain specified performance levels under flexible power system operation.

The delivery of this flexibility is out with the scope of this chapter and will be dealt with in chapters 4 and 5 as part of an adaptive protection strategy. The extent of possible/required flexibility and the system stimuli defining the boundaries of robust behaviour will also be examined. This will be taken a step further and formulated in chapter 6 such that effective verification of flexible behaviour is possible.

3.6.3 Robustness in protection measurement algorithms

The previous section addressed the robustness of protection system behaviour. However, this does not take into account variations in the measurements made by the protection system. Obtaining measurements, with an acceptable error defined by the application is a prerequisite for correct protection operation. For example, the accurate measurement of frequency for some protection applications is critical to the correct operation to these functions. This is especially the case for off-nominal frequency measurements and those containing harmonic distortions [45]. Advanced filtering techniques have been used in addition to flexible measurement windows to enhance the robustness of information gathering by the measurement stage of the protection system.

As shown in section 3.5, the disparity in LOM protection performance between different manufacturer offerings was mainly attributed to the frequency measurement algorithms' different implementations. This is evidence to the lack of an appropriate level of robustness against a varied set of events (i.e. true loss of mains and remote disturbances with different initial conditions). Flexible alteration in the measurement algorithms' dynamic response to frequency changes can be used to address this problem. However, the main challenge here lies in choosing an appropriate flexible course of action during the occurrence of an event.

3.7 Chapter summary

This chapter reviewed the impact the variable power system topology, increased utilisation of DER, ubiquitous FACTS and more frequent occurrences of system wide disturbances have on the performance of existing protection practices. This revealed a wide range of performance issues that affect the sensitivity, selectivity, stability and speed of protection. The power system is not necessarily left in an unprotected state. Nevertheless, the deterioration in protection performance levels have been shown to lead to unnecessary loss of supply and in extreme cases the onset of cascade tripping events which can lead to blackouts.

Further to the effects these aforementioned contributors have, the increasing trend of flexible power system operation presents its own array of challenges. Flexible power system operation leads to variability in conditions as seen by the protection systems. And consequently increases the risk of exposing their performance as they rely on fixed settings which are not designed to cope with such variable system conditions. To support the understanding of this impact, detailed simulations and relay testing were conducted to examine the performance of distance protection and loss of mains protection under select flexible power system operation conditions.

An evaluation of distance protection performance was conducted to ascertain the impact that QBs have on this scheme. The analysis revealed that the distance protection can suffer a reach error of up to 5.68Ω. This extent of impact depends on the QB mode and tap position where the worst case scenario occurs for phase to phase faults. There is no evidence that operating grid QBs through a national coordinated control strategy has an additional impact on the reach of the relays.

The assessment of loss of mains protection performance revealed not only the disparity of performance between the different manufacturer relays, but also the effect that the type of generation has on the sensitivity and stability. Industry recommended ROCOF settings of 0.15Hz/s were shown to be prone to unstable LOM operation. Improved stability is better achieved through the introduction of time delays rather than raising the pick-up threshold which compromises sensitivity. LOM protection was shown to be largely ineffective in the secure operation of inverter-interfaced DG especially when fault ride-through is required. In other words, when LOM mal-operates due to remote faults, the inverter-interfaced DG is disconnected denying the grid of this resource. An incremental improvement in LOM performance can be obtained by applying the compromise settings proposed in the chapter. This is seen as a short term solution to the performance issues experienced which is favourable by network operators as opposed to the deployment of communications based LOM protection or indeed unproven islanding detection techniques.

In light of the performance issues reviewed and demonstrated, the chapter examined whether achieving robust protection behaviour is sustainable under flexible power system operation. It was revealed that flexible protection behaviour is necessary to sustain the required robustness. Although seen as conflicting objectives, robustness and flexibility can indeed coexist by dynamically changing the protection behaviour in a discrete manner to reflect prevailing power system conditions. Moreover, this flexibility must be exhibited in varying degrees by constituent elements of the protection scheme (i.e. measurements, protection characteristic and scheme logic). Ways to achieve flexible protection operation through adaptive relaying will be investigated in the next chapter.

3.8 References

[1] J. De La Ree, Y. Liu, L. Mili, A. G. Phadke, and L. DaSilva, "Catastrophic Failures in Power Systems: Causes, Analyses, and Countermeasures," *Proceedings of the IEEE,* vol. 93, pp. 956-964, 2005.

[2] S. H. Horowitz and A. G. Phadke, "Blackouts and relaying considerations - Relaying philosophies and the future of relay systems," *Power and Energy Magazine, IEEE,* vol. 4, pp. 60-67, 2006 2006.
[3] F. Coffele, C. Booth, G. Burt, C. McTaggart, and T. Spearing, "Detailed Analysis of the Impact of Distributed Generation and Active Network Management on Network Protection Systems," in *CIRED 2011*, 2011.
[4] A. Dysko, G. M. Burt, S. Galloway, C. Booth, and J. R. McDonald, "UK distribution system protection issues," *Generation, Transmission & Distribution, IET,* vol. 1, pp. 679-687, 2007.
[5] D. Tholomier and A. Apostolov, "Adaptive protection of transmission lines during wide area disturbances," in *Power Systems Conference and Exposition, 2009. PSCE '09. IEEE/PES*, 2009, pp. 1-7.
[6] E. M. Davidson, M. J. Dolan, G. W. Ault, and S. D. J. McArthur, "AuRA-NMS: An autonomous regional active network management system for EDF energy and SP energy networks," in *2010 IEEE Power and Energy Society General Meeting*, 2010, pp. 1-6.
[7] A. T. Ohara and C. S. Takiguchi, "Automatic restoration system," in *Transmission and Distribution Conference and Exposition: Latin America, 2004 IEEE/PES*, 2004, pp. 681-685.
[8] T. Funabashi, K. Koyanagi, and R. Yokoyama, "A review of islanding detection methods for distributed resources," 2003, pp. 6-pp. Vol.2.
[9] R. S. Kunte and G. Wenzhong, "Comparison and review of islanding detection techniques for distributed energy resources," in *Power Symposium, 2008. NAPS '08. 40th North American*, 2008, pp. 1-8.
[10] M. A. Zamani, T. S. Sidhu, and A. Yazdani, "A Protection Strategy and Microprocessor-Based Relay for Low-Voltage Microgrids," *IEEE Transactions on Power Delivery,* vol. 26, pp. 1873-1883, 2011.
[11] R. M. Tumilty, M. Brucoli, G. M. Burt, and T. C. Green, "Approaches to network protection for inverter dominated electrical distribution systems," in *Power Electronics, Machines and Drives, 2006. PEMD 2006. The 3rd IET International Conference on*, 2006, pp. 622-626.
[12] Alstom, *Network Protection and Automation Guide - Protective Relays, Measurement and Control*, 2011.
[13] CIGRÉ. W.G. B5.15, "Modern Distance Protection Functions and Applications," 2008.
[14] F. Coffele, C. Booth, A. Dysko, and G. Burt, "Quantitative analysis of network protection blinding for systems incorporating distributed generation," *Generation, Transmission & Distribution, IET,* vol. 6, pp. 1218-1224, 2012.
[15] S. Sirisophonwattana and S. Chaitusaney, "Maximization of Distributed Generation with consideration of Fuse-Recloser coordination," in *2011 8th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, 2011, pp. 857-860.
[16] E. Sortomme, G. J. Mapes, B. A. Foster, and S. S. Venkata, "Fault analysis and protection of a microgrid," in *Power Symposium, 2008. NAPS '08. 40th North American*, 2008, pp. 1-6.

[17] I. F. Abdulhadi, G. M. Burt, A. Dysko, R. Zhang, and J. Fitch, "The evaluation of distance protection performance in the presence of Quadrature Boosters in support of a coordinated control strategy," in *Developments in Power System Protection (DPSP 2010). Managing the Change, 10th IET International Conference on*, 2010, pp. 1-5.

[18] M. Khederzadeh and T. S. Sidhu, "Impact of TCSC on the protection of transmission lines," *Power Delivery, IEEE Transactions on,* vol. 21, pp. 80-87, 2006 2006.

[19] L. F. Santos and P. M. Silveira, "Evaluation of Numerical Distance Protection Algorithms for Series Compensated Transmission Lines," in *Transmission & Distribution Conference and Exposition: Latin America, 2006. TDC '06. IEEE/PES*, 2006, pp. 1-6.

[20] T. S. Sidhu and M. Khederzadeh, "TCSC impact on communication-aided distance-protection schemes and its mitigation," *Generation, Transmission and Distribution, IEE Proceedings-,* vol. 152, pp. 714-728, 2005 2005.

[21] M. A. Zorrozua Arrieta, J. F. Miñambres Argüelles, M. Sanchez Benito, B. Larrea Jaurrieta, and P. Infante Otamendi, "Influence of a TCSC in the behaviour of a transformer differential protection," *Electric Power Systems Research,* vol. 74, pp. 139-145, 2005.

[22] H. J. Altuve, J. B. Mooney, and G. E. Alexander, "Advances in series-compensated line protection," in *Protective Relay Engineers, 2009 62nd Annual Conference for*, 2009, pp. 263-275.

[23] J. Kincaid, I. Abdulhadi, A. S. Emhemed, and G. M. Burt, "Evaluating the Impact of Superconducting Fault Current Limiters on Distribution Network Protection Schemes," in *Universities' Power Engineering Conference (UPEC), Proceedings of 2011 46th International*, 2011, pp. 1-5.

[24] S. Orpe and N.-K. C. Nair, "State of art of fault current limiters and their impact on overcurrent protection," in *Energy Society General Meeting (PES)*, 2009, pp. 1-5.

[25] A. Atputharajah and T. K. Saha, "Power system blackouts - literature review," in *Industrial and Information Systems (ICIIS), 2009 International Conference on*, 2009, pp. 460-465.

[26] H. Seyedi and M. Sanaye-Pasand, "New centralised adaptive load-shedding algorithms to mitigate power system blackouts," *Generation, Transmission Distribution, IET,* vol. 3, pp. 99-114, 2009.

[27] D. C. Elizondo, J. de La Ree, A. G. Phadke, and S. Horowitz, "Hidden failures in protection systems and their impact on wide-area disturbances," in *Power Engineering Society Winter Meeting, 2001. IEEE*, 2001, pp. 710-714 vol.2.

[28] Y. Fang, A. P. S. Meliopoulos, G. J. Cokkinides, and Q. B. Dam, "Effects of Protection System Hidden Failures on Bulk Power System Reliability," in *Power Symposium, 2006. NAPS 2006. 38th North American*, 2006, pp. 517-523.

[29] ABB, *Self supervision techniques, 670 series Principles and functions*: ABB, 2009.

[30] P. Jarman, P. Hynes, T. Bickley, A. Darwin, H. Hayward, and N. Thomas, "The Specification And Application Of Large Quadrature Boosters To Restrict Post-Fault Power Flows," in *CIGRÉ Session 2006*, 2006.
[31] M. Zhu and A. Dale, "Application and modelling of quadrature boosters for the HV transmission system," in *Power System Technology, 1998. Proceedings. POWERCON '98. 1998 International Conference on*, 1998, pp. 923-927 vol.2.
[32] AREVA, *Power Transformers: Fundamentals and Expertise*: AREVA T&D, 2008.
[33] NGET, "National Grid Substation Commissioning Course - Quadrature Boosters Module," 2008.
[34] M. J. Heathcote, *J & P Transformer Book*: Newnes, 2007.
[35] M. Belivanis and K. R. W. Bell, "Coordination of phase-shifting transformers to improve transmission network utilisation," in *Innovative Smart Grid Technologies Conference Europe (ISGT Europe), 2010 IEEE PES*, 2010, pp. 1-6.
[36] P. K. Dash, A. K. Pradhan, G. Panda, and A. C. Liew, "Digital protection of power transmission lines in the presence of series connected FACTS devices," in *Power Engineering Society Winter Meeting, 2000. IEEE*, 2000, pp. 1967-1972 vol.3.
[37] NGET. (2011). *National Electricity Transmission System (NETS) Seven Year Statement*. Available: http://www.nationalgrid.com/uk/Electricity/SYS/current/
[38] D. S. Ouellette, W. J. Geisbrecht, R. P. Wierckx, and P. A. Forsyth, "Modelling an impedance relay using a real time digital simulator," in *Developments in Power System Protection, 2004. Eighth IEE International Conference on*, 2004, pp. 665-668 Vol.2.
[39] N. Tleis, *Power Systems Modelling and Fault Analysis: Theory and Practice*: Newnes, 2008.
[40] IEC, "IEC 60255: Measuring relays and protection equipment," ed, 2010.
[41] Electricity Networks Association, "ER G59/2: Recommendations for the Connection of Generating Plant to the Distribution Systems of Licensed Distribution Network Operators," 2010.
[42] IEEE, "IEEE Application Guide for IEEE Std 1547, IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems," 2009.
[43] Electricity Networks Association, "ENA ETR 139: Recommendations for Setting of Loss of Mains Protection Relays," 2009.
[44] S. Kubisch, R. Hecht, R. Salomon, and D. Timmermann, "Intrinsic Flexibility and Robustness in Adaptive Systems: A Conceptual Framework," in *Adaptive and Learning Systems, 2006 IEEE Mountain Workshop on*, 2006, pp. 98-103.
[45] A. J. Roscoe, I. F. Abdulhadi, and G. M. Burt, "P-Class Phasor Measurement Unit algorithms using adaptive filtering to enhance accuracy at off-nominal frequencies," in *2011 IEEE International Conference on Smart Measurements for Future Grids (SMFG)*, 2011, pp. 51-58.

4 Delivering Flexible Protection Schemes with Enhanced Performance using an Adaptive Protection Philosophy

4.1 Chapter methodology and contributions

Adaptive protection is an effective means of delivering the flexibility required for improving protection scheme performance. Dynamic alterations of protection IEDs or scheme configurations to suit prevailing power system conditions can deliver this improvement. This is especially true with a power system that is increasingly exhibiting complexity and variability in operating conditions. The validity of this hypothesis depends on understanding the extent to which adaptive protection functionality can provide the required flexibility in performance, and the required means of achieving that.

The previous chapter presented and demonstrated the performance issues associated with some of the existing protection arrangements under existing and future power system operational conditions. It also discussed the need for flexibility in protection functionality to achieve robust performance under varying system conditions.

This chapter investigates the suitability of adaptive protection as a means of achieving the required flexibility in protection functionality. The concept of adaptive protection will be discussed in this chapter along with the main protection system elements used to achieve protection functionality. The state of the art of adaptive protection techniques will also be reviewed. This review will cover those techniques which utilise intelligent systems, transient signal analysis, fuzzy logic and heuristic optimisation to achieve improved protection sensitivity or scheme coordination.

Adopting an adaptive protection strategy to replace or complement existing practices comes with its own set of challenges. These are either technical or institutional barriers which hinder the integration of adaptive functionality with existing arrangements or utility policies and procedures. These challenges will be discussed and those challenges specific to different protection behaviour adaptation techniques will be detailed. However means of overcoming these challenges will be discussed and demonstrated in the following chapter.

Finally, the distance protection performance case study in the previous chapter will be used as a basis to show how settings groups can be best calculated and used as a means of adapting the used distance protection functionality and improving its selectivity. The engineering implementation of the settings groups and setting selection strategy will be detailed in the following chapter.

The main contributions of this chapter are:

- Defines the scope for the use of adaptive protection functionality. This entails identifying the operational conditions of the power system where adaptive functionality is deemed suitable.
- Identifies the technical and institutional challenges associated with adopting an adaptive protection philosophy. This involves identifying implementation challenges associated with novel adaptive protection approaches proposed in the literature.
- Proposes a procedure for calculating and assigning protection settings groups for relays which offer a limited set of settings groups. This will be used for the adaptive distance protection scheme developed in the remainder of this thesis which takes into account the impact a QB has on the reach of plain distance schemes.

4.2 Adaptive protection concept review

Adaptive protection is not a new protection philosophy. However, in its true sense, its application remains confined to academic work and was first proposed in [1]. The most widely used definition of adaptive protection can be found in [2]:

"Adaptive protection is a protection philosophy that permits and seeks to make adjustments automatically in various protection functions to make them more attuned to prevailing power system conditions".

This definition identifies the two main characteristics of an adaptive protection philosophy – that is the adjustment of the protection scheme functions or configuration and the automatic nature of this adjustment. Both characteristics serve the objective of matching the protection scheme or behaviour to the prevailing power system conditions in order to improve the protection performance. Therefore, it is necessary for the adaptive protection scheme to monitor the power system to determine its state and adjust its configuration accordingly. In light of this definition, the following subsections will discuss the resulting requirements for adaptive protection schemes.

4.2.1 Identification of prevailing power system conditions

It is necessary to define what a prevailing power system state means from a protection system perspective. Consider a transmission line with series compensation for instance. As discussed in chapter 3, distance protection applied to this line can experience zone reach issues. This is also directly influenced by the mode of operation of the series compensation, the level of compensation and the relative positions of fault and compensation apparatus to the protection relay. Therefore it can be concluded that in this instance, the prevailing power system conditions are determined by the state of the series compensation. A further example would be identifying islanded or grid-connected operation of sections of the distribution network (or microgrids). Chapter 3 also discussed the impact of islanding on the performance of overcurrent protection schemes especially when inverter-interfaced DER is

predominant in a microgrid. This means that that the prevailing power system condition, in this case, is related to the connection mode of the microgrid and the DER type and activity. There remains an element of uncertainty, however, related to the fault nature and location. Ideally, knowledge of this greatly enhances the knowledge of the system conditions. However, characterising the fault conditions to serve adaptive protection functionality can prove difficult especially due to the tight time frames involved in decision making.

It is then clear that from a protection perspective, that knowledge of the prevailing power system condition is tied with the knowledge of the source and extent of performance impact network conditions has on a specific protection function. Consequently, adaptive protection functionality will need to infer these prevailing conditions by making the appropriate direct or derived measurements. Prevailing power system conditions, from a protection standpoint, can be inferred from information obtained from measurements made during fault conditions or after the occurrence of operational events pre-fault conditions. System information obtained in both categories can be potentially used to adapt the protection system functionality. However, there are risks and challenges involved in their use when attempting to alter the behaviour of the protection.

Consider the series compensation example once again. The knowledge of level of compensation can be directly used to alter the zone reach of the distance relay and avoid potential reach issues. However, mal-operation of the directional element cannot necessarily be dealt with in the same manner. Since voltage and current inversion are influenced by the fault location, it is difficult to initiate any corrective adaptive behaviour prior to the fault conditions. Therefore, any adaptive protection actions designed to deal with this condition must rely on the information gathered during the fault onset and development. This means that relying on pre-fault information is largely ineffective in dealing with any protection performance impact caused by fault location or type. Conversely, attempting to adapt protection behaviour during fault conditions can be seen as a risky strategy. Measurements during fault conditions may not

provide a completely reliable view of the system status especially when protection is expected to operate within very small timescales. Furthermore, dynamic changes to the protection system during a fault event can in itself be seen as a cause of mal-operation especially if obtained information is misinterpreted by the adaptive scheme. Relying on pre-fault information to adapt the protection functions will usually involve the use of communications to obtain the relevant measurements from remote information sources. Having said that, communications can be seen as a vulnerability if it is to fail and the adaptive protection scheme has no fall back strategy to cope with it.

4.2.2 Adaptable protection functions

Given the capabilities of existing relaying platforms, there are three possible approaches to adapt the behaviour of the protection functionality in accordance with prevailing power system conditions:

- Modification of active settings.
- Use of programmable scheme logic (PSL).
- Inherent protection element adaptive behaviour.

Modification of active settings is seen as the most direct way of altering protection behaviour. Furthermore, this method is more understood by protection scheme users. Modifying protection settings can be approached in two ways – selection of active settings from a set of pre calculated settings groups or the calculation of settings as and when necessary while the scheme is in service then applying these settings to the appropriate protection IEDs.

The first method of settings modification may be seen as less flexible compared to the second one due to the restriction of limited available settings to choose from. The risk in this case is the potential lack of an appropriate settings group. That said, a limited number of settings groups may be appropriate to reasonably cover for all foreseen power system conditions as will be seen in the case study in 4.5. Furthermore, relying on settings groups can facilitate the validation of the adaptive scheme since there is a known set of possible settings. Commercial protection IEDs provide several settings groups (typically 4-6 groups) that can

be easily switched between remotely. Calculating protection settings on the fly (or online) would be conducted in a similar manner to that performed by an engineer (e.g. an over current protection scheme grading study). An algorithm performing such functionality automatically requires several input measurements, an equivalent power system model and protection setting constraints to perform the calculations.

A PSL can be setup in such a way that the output from a protection scheme can be influenced by system conditions. Binary indications from primary system plant can be used as additional inputs to the scheme logic. Also, more elaborate scheme logic circuits can be developed to deal with a wider range of system operating conditions as opposed to what is being used at the moment. None of the existing commercial offerings allow changing between different PSL circuits in a similar manner to settings groups. However, the need for such functionality is yet to be demonstrated. As protection IEDs become more feature rich and offer more advanced functionality, accurate documentation of PSL becomes ever more important. This is especially challenging when attempting to compare PSL between devices from different vendors and indeed under adaptive protection operation.

The approaches described so far can be used to adapt the behaviour of existing protection scheme functions without changing the protection element functionality (e.g. overcurrent, distance elements). Conversely, changes to the existing functionality can be used to adapt scheme behaviour. This results in introducing new protection elements or modifying existing elements. Examples of such functionality are discussed in section 4.3. Should some of these techniques rely on settings to determine their operation, then modifying these settings can still be a valid means of adapting the behaviour of the scheme.

4.2.3 Automatic adjustments of protection functions

Having no operational user intervention is a requirement for a functioning adaptive protection scheme. Therefore, it is necessary to provide some form of functionality (logic) which bridges the gap between the identification of prevailing system conditions and the appropriate adaptive scheme action.

This gap can be filled with functionality which identifies the extent of impact that a change in network conditions has on the performance of the protection scheme operating with some given setting. This and the minimum performance requirements are used to inform the decisions made by the adaptive setting logic (settings group selection or online calculation). This exchange of information between different functional elements should be defined in terms of content and frequency of occurrence. These are defined in the following chapter when an architecture encompassing these functions is developed. Figure 4-1 illustrates the functionality of an adaptive protection scheme based on the definition above. An adaptive protection action is initiated by a change in power system prevailing conditions. This needs to be monitored and its impact on the performance of the protection at the active setting identified. Then a suitable course of action (in the form of setting change or otherwise) is sanctioned.

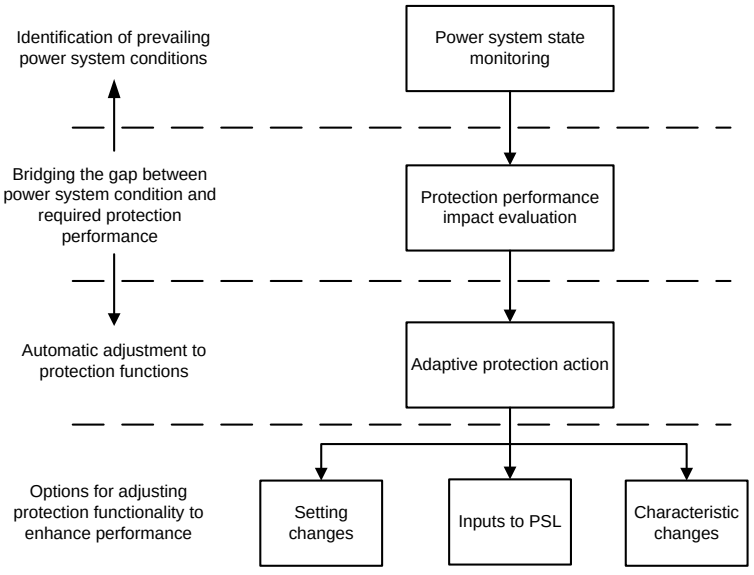

Figure 4-1 Adaptive protection scheme composition

4.3 Review of techniques to achieve adaptive protection functionality

As discussed in the introductory section of this chapter, the examination of adaptive protection schemes proposed in the literature will be limited to those functions which aim to improve scheme sensitivity or coordination. It should be emphasised that coordination in this case encompasses ensuring the selective operation of the protection scheme. Other examples exist to address protection stability and speed of operation, but the scope of the first set of examples best matches the scope of the thesis and indeed the developed adaptive distance protection scheme. The review will not delve into the problems that these adaptive schemes address as the need for adaptive protection has already been established in the previous chapter. Nor will it discuss the intricacies of the techniques used as this is out with the scope of the thesis. The schemes reviewed fall under one of the following categories in terms of techniques used to achieve adaptive functionality:

- Artificial neural networks (ANN): neural networks are used to recognise patterns in measured power system quantities that reflect its prevailing operational state [3]. Based on this pattern recognition, a decision can be made to alter the behaviour of the protection accordingly. An ANN requires offline training to tune its functionality [4].
- Optimisation techniques: linear or heuristic optimisation techniques [5, 6] are used to achieve an objective function which usually aims to minimise operating time or maximise selectivity based on network conditions.
- Fuzzy logic: a fuzzy membership function is used to determine the primary system state [7] which affects the setting of the adaptive protection.
- Data mining: offline analysis of power system data is used to classify its operation into states (e.g. islanded and grid connected network). This analysis is then used to create a 'decision-tree' logic for online use to

infer the state of the system and feed it into the adaptive protection algorithm for decision making.

- Multi agent systems (MAS): Distributed 'intelligent' functions operate cooperatively over a communications network to achieve a performance objective [8] which is usually related to the coordination of a multi-relay scheme.
- Expert systems: the expertise of a protection engineer or power system operator is captured in an algorithm to provide decision making functionality [9]. This aims to alter the protection behaviour to deal with varied power system operating conditions, the same way an expert would do.
- Numerical techniques: these techniques usually implement an online form of protection setting calculations that are normally performed offline [10, 11]. Other approaches involve the use of multiple prioritised objectives to inform the operation of the protection functions [12].
- Hybrid techniques: these use a combination of two of the above techniques to adaptive the protection behaviour [13].

4.3.1 Adaptive protection to improve scheme sensitivity

As discussed in the previous chapter there are situations when the pick-up threshold of the protection is not sufficiently tuned to deal with varied power system conditions such as varied fault levels, distinguishing between islanding and grid connected states or detecting resistive faults. To this end, a number of adaptive protection schemes have been proposed to deal with these situations.

The use of ANN has been proposed to detect resistive faults and alter the tripping logic of distance protection schemes [14]. Self-organising ANNs are used to alter the operating characteristic of the distance protection such that a temporary extension that encompasses resistive fault impedances is achieved. A common problem with ANN based adaptive schemes is that the response is always specific to the training data set for the ANN. Therefore the impact of transducer errors or different fault impedances is not fully understood or catered for.

Adaptive scheme examples based on numerical techniques are plentiful. The underlying principle of operation however remains largely similar – that is the use of power system measurements as inputs to a short circuit calculation or state estimation which is then used to tune the protection accordingly. In [15], generator infeeds in a multi terminal transmission circuit are measured to alter the reach of zone 2 distance protection. Short circuit simulations are performed offline calculate the seen impedance by zone 2 under different infeed levels. Based on the results, the reach of zone 2 is minimised to avoid overreaching into adjacent lines. In [16], another numerical algorithm is proposed to deal with the reach error effect mutual coupling has on distance protection. The measured impedance is compensated based on the current flowing in the parallel circuit. A number of states are defined according to the loading of the parallel circuit and fault impedance locus. These determine the appropriate action for the distance protection scheme. An adaptive load encroachment algorithm has been proposed in [11]. Based on system wide measurements, the relay at most risk of load encroachment is identified. This is used to apply an anti-encroachment zone (AEZ). Then a simple binary logical operation is performed to combine the distance characteristic and AEZ responses to a fault locus to produce the trip command.

Data mining is increasingly finding new applications in power systems [17, 18]. In [19], data mining is used as a means to bias the operation of existing protection schemes towards dependability or security according to power system conditions (i.e. normal or stressed operations). Data mining is used to classify the power system measurements that reflect normal or stressed operation. A voting logic based on a decision tree derived from the classification process is introduced between feeder protection relays and the final trip command. Whenever significant changes are made to the network the logic must be revised. So it is unclear how the logic would perform if the system topology changed often or its dynamics change due to changes in connected generation.

4.3.2 Adaptive protection to improve scheme coordination

Coordination in a multi-relay scheme is an important issue when their behaviour is being altered dynamically. There are a number of adaptive protection techniques that ensure coordination is maintained. For instance, optimisation techniques have been used to this effect. In [20], particle swarm optimisation (PSO) has been used to coordinate overcurrent protection relays using the grading margins as a constraint. Several hundreds of iterations are usually required to reach convergence. It is not clear whether the computing requirements and time to achieve convergence are suitable for an online application of the method to adapt the overcurrent settings. Another optimisation method based on genetic algorithm (GA) is proposed in [21] to alter the operation of load shedding schemes. The amount of load shed is reduced with each stage to minimise customer interruptions.

Numerical approaches have also been used to achieve adaptive protection. Both [12] and [22], propose an approach to load shedding using multiple criteria. A combination of bus voltage calculations and rate of change of frequency measurements determine the load priority and speed of disconnection to best serve the system stability. Although high-speed communications are a prerequisite for the effective operation of the scheme, no specific requirements have been given. At the distribution level, numerical approaches rely on calculating short circuit levels for a given network configuration and applying the appropriate settings to the overcurrent relays as in [23].

The nature of MAS lends itself to address the coordination problem since it relies on peer to peer communication to achieve an overall objective. A MAS based load shedding scheme has been proposed in [24]. Loads are continuously monitored and when the need for disconnection arises, the scheme prioritises attempts to minimise the amount of load disconnected. Different agents take the responsibility of system monitoring. In [25], overcurrent relays form part of a MAS to coordinate the settings of overcurrent relays in the presence of DG. The literature, however, tends to focus on the MAS architecture as opposed to the intricacies of the coordination algorithms. Finally hybrid techniques such as that

proposed in [9] rely on expert system and fuzzy logic to determine the faulted section of a network. Initial operation of protection elements surrounding the fault is used to define a search region. The hybrid approach is then used to zoom in on the faulty feeder.

4.3.3 Shaping the research direction for adaptive protection

It is clear that there is no shortage of advanced adaptive protection schemes proposed in the literature that rely on intelligent systems techniques or otherwise to achieve improved performance levels. But why has none of these or many others previously proposed have never been deployed in the real power system despite a clear need for such improved performance and a clear advantage offered by these proposals? In fact therein lies the problem with adaptive protection. The problem of its applicability and not the problem of gaining an 'X' performance enhancement for a 'Y' network that is operated under 'Z' conditions. Furthermore, with the exception of MAS based schemes, there is a lack of consideration to the scalability and future proofing of these schemes. What should be done when the scope of the adaptive scheme needs to be expanded to encompass more relays? What if more DG has been added to the network? How does the utility manage and maintain the settings of these schemes? More importantly, what if these schemes do not rely on crisp settings in the conventional sense?

So it seems that the performance problems facing static protection (that is uncertainty and variability in the power system) remain so with some of the advanced techniques being proposed. Some of the performance problems are being effectively addressed. But the problem of being able to cope with system variability keeps recurring even with the use of adaptive techniques. Perhaps problem of producing a truly universal adaptive scheme is an unwieldy one. To this end, the remainder of this thesis will not focus on adding to the pool of existing adaptive algorithms, but it will attempt to understand the bigger picture issues related to adaptive protection, thus establishing the scope, requirements and approaches that make adaptive protection a credible solution.

4.4 Challenges to adopting adaptive protection

Adaptive protection can offer performance advantages compared with conventional schemes. However, there are technical and institutional challenges that must be overcome beforehand. This section discusses the main challenges associated with the adoption of an adaptive protection philosophy. Three main challenges are discussed in this section.

4.4.1 Integration with existing protection arrangements

An overhaul of existing protection arrangement to accommodate adaptive functionality is not an attractive option. This is especially the case with older substation installations. New substations may be more suited for introducing adaptive functionality. That said, there must be an assessment of the impact such introduction can have on the wider system protection. This includes the requirement for coordination with adjacent circuits and/or other protection functions as well as any requirement to exchange information with existing substation systems.

Communication standards such as IEC 61850 have created a vehicle to facilitate the interoperability between protection functions from different vendors and potentially the interchangeability of those functions. Similarly, adaptive protection functions to be integrated into existing protection arrangements must adhere to interfaces offered by existing functions. As discussed in section 4.2.1, inferring the system state by an adaptive scheme may require access to remote signalling to determine primary plant status. If this information is to be made available from the existing substation communication network (LAN), then the integration exercise becomes easier. More issues lie in furnishing the adaptive protection functionality with signals from remote substations. The absence of suitable communication infrastructure will then need to be remedied. Factors affecting the choice of a suitable communications infrastructure include the required reliability and timeliness of the information a communications link can offer. The change of settings will take a finite time to achieve which will be added to the time delays caused by communications overhead. This must be considered in the context of the application. It may be

the case that critical circuits (e.g. major transmission corridors) will have more stringent information timeliness requirements.

4.4.2 Adaptive scheme testing

Testing of protection schemes has always been an important aspect in a scheme's lifecycle. The testing of adaptive protection schemes is not different and in fact is of greater importance. This is mainly due to the increased complexity in scheme behaviour due to the introduction of adaptive functions. The behaviour of the scheme is perceived to be less deterministic especially with the use of some of the advanced techniques described in section 4.3. Furthermore, adaptive protection functions respond to an extended range of events. In other words the testing of the scheme functionality should not be limited to verifying the response of the protection elements to faults. Tests must also verify the correct change of settings (or scheme configuration) in response to changes in prevailing network conditions. Generally speaking, tests performed on adaptive protection schemes must complement those defined in international standards (e.g. IEC 60255 [26]) but not replace them. More emphasis will be on stimulating the adaptive protection logic rather than verifying the performance of conventional protection elements. The following two chapters discuss the requirements for testing and different testing methods for adaptive protection schemes and demonstrated developed testing methodologies using the adaptive distance protection algorithm.

4.4.3 Inadequacy of utility policies and procedures

A typical utility protection scheme specification for a distance protection scheme can take the following form:

- ✓ Main 1 protection: Unit type sensitive for minimum in zone fault current and for all types of faults with a minimum fault resistance of 100Ω.
- ✓ Main 2 protection: Non-unit type distance protection (Mho or quadrilateral) with 80% zone 1 reach and 0s

time delay, 150% zone 2 reach and 0.5s time delay and 220% zone 3 reach and 1s time delay.

- ✓ Back-up protection: Standard inverse overcurrent protection for phase and earth faults set to coordinate with main 1 and 2 protection.

Distance protection zones 2 and 3 are not to detect faults onto 275kV feeders. Main 1 and 2 protection scheme logic is to operate in a 1 out of 2 configuration. Main 2 relay characteristic angle (RCA) is to be set in accordance with relay manufacturer instructions.

It can be noted from the above policy excerpt that some of the specifications can be lose in terms of specifying minimum performance and relying on the discretion of the manufacturers. This is perfectly adequate for well-established protection practices. However, if further complexity is to be added to the substation in the form of adaptive protection schemes, then the specifications will need to be improved (i.e. better quantified) to reflect the impact of such schemes on existing operational practices.

Furthermore, the utility must manage the transition from conventional protection schemes to those with adaptive features without jeopardising the stability of the system. Furthermore, adaptive schemes must be able to coexist with legacy schemes without affecting their coordination. This is in addition to the testing and commissioning requirements for each type of scheme. All of these concerns are not addressed by existing utility policies and must be addressed by defining additional functional and performance requirements and acceptable testing procedures in light of relevant standards (e.g. IEC 60255 [26]) if possible.

4.5 Using settings groups to enhance distance protection performance in QB presence

The first step in realising an adaptive protection scheme based on settings group changes is to determine these settings groups for the given application. In this case, the problem of distance protection reach error caused by QBs and introduced in the previous chapter is revisited. The extent of reach error previously quantified will be used to calculate suitable settings groups while ensuring that mis-coordination with adjacent lines does not occur. Furthermore, the calculation will take into account the limited number of settings groups that relays offer at the moment. However, a method to overcome this limitation is also proposed.

4.5.1 General strategy for the adaptive distance protection scheme

The full design and implementation details of the adaptive distance protection scheme dealing with the presence of the QB on a transmission circuit will be presented in the following chapter. Nevertheless, for the purposes of clarity, a general description of the scheme functionality will be discussed in this section.

As identified in the previous chapter, the distance protection can under reach when the QB is engaged into the circuit. Over reach is also possible, when the QB is bypassed while the protection is set to compensate for its presence to protect the remote busbar. The affected zones of protection will then need to be adjusted (reach expanded, reduced or changes blocked) accordingly with the aid of status indications obtained from the QB controller. The flowchart in Figure 4-2 illustrates the approach to the setting changes.

The adaptive scheme must determine the extent of reach error for an active QB state. This is based on the relation derived from the reach error analysis in chapter 3 and was shown to be deterministic. The reach error magnitude $|\Delta Z|$ is compared to a pre-calculated threshold δ over which an under reach is considered unacceptable. Since operating the QB in a bucking mode results in more under reach than when a boosting mode is employed, settings group 4 (SG4) will provide a larger reach than setting group 3 (SG3). Furthermore,

expanding the reach of the affected protection zones while a short adjacent transmission line exists can result in zone 2 mis-coordination (as discussed in chapter 2). Therefore, the default setting is preferred in this case (SG1). Alternatively, zone 2 of the remote relay can be extended in line with the local relay zone extension to avoid mis-coordination. The first method is preferred to minimise potential mis-coordination with relays downstream of the short adjacent line. Finally, load encroachment on heavily loaded transmission lines can present a risk of mal-operation especially for zone 3. Extending the zone to cope with the presence of a QB can increase this risk. Therefore, similar to the mis-coordination case, the default settings group is activated during this situation. Load blinders can be used to minimise load encroachment. But with adaptive extensions of the zones, the load blinders must also be adjusted.

The approach to changing the settings depicted in Figure 4-2 reflects the adaptive protection scheme composition shown previously in Figure 4-1. This means that it consist of three main functional stages:

- Power system state monitoring: the state of the QB and circuit is determined through the interpretation of related status measurements.
- Protection performance impact evaluation: the impact of QB state on distance protection reach is determined.
- Adaptive protection action: the new protection settings are selected and applied to improve the performance where necessary.

This sequence of functions is more formally defined in chapter 5 when the adaptive protection architecture is introduced and corresponding functions are mapped to the architecture.

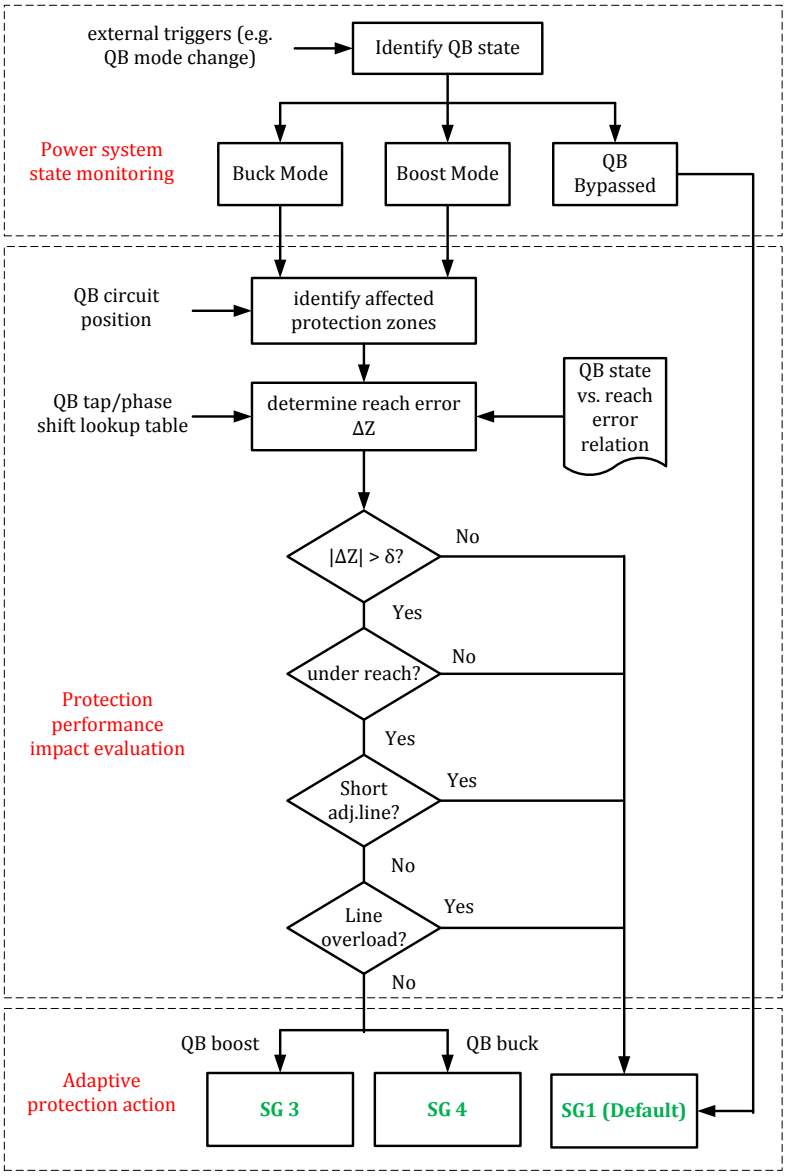

Figure 4-2 Adaptive distance protection general strategy

4.5.2 Settings group calculation and mapping to power system states

The factors affecting the distance protection reach and setting constraints are determined first:

- Mode of QB operation and its tap positions.
- Minimum distance zone reaches based on minimum performance criteria specified in the utility protection policy.
- Maximum allowable zone reaches taking into account coordination constraints with adjacent lines.

Figure 4-3 shows the measured impedance locus for different phase to phase fault locations and for different QB operational modes and tap positions (detailed results can be found in chapter 3). Taps 1, 3 and 5 are used where tap position 1 provides the worst case scenario. The busbar names indicate the substation names and the faults are positioned between HIGM and RATS substations at 0%, 30%, 50%, 70% and 100% line length. The distance protection zones depicted are zones 1-3 at WBUR substation and zones 1-2 at HIGM substation. The purpose of showing the protection zones at HIGM is to illustrate potential coordination issues.

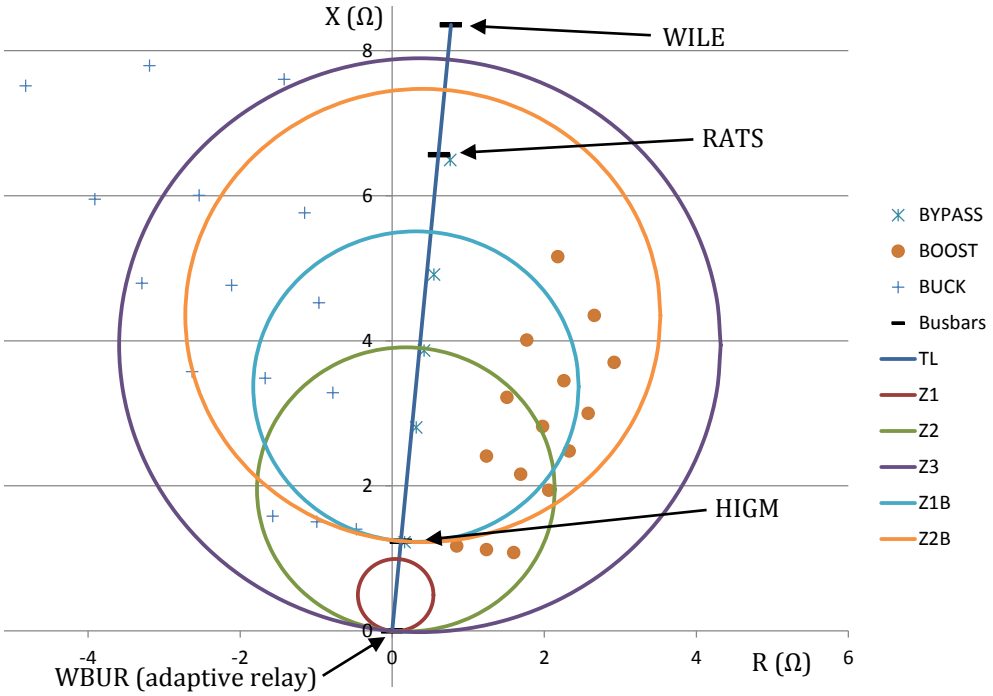

Figure 4-3 Phase to phase fault impedance locus mapping on Mho diagram with different QB modes, tap positions and fault positions

Figure 4-4 shows an extended zone 2 (AZ, dotted zone) to provide coverage for worst case under reach when the QB is operated in boost mode. The default protection zones are left in the figure for comparison. All reach values are quoted at the transmission line angle of 84.7˚. The zone reach in this situation would be 4.3Ω – an increase of 9.7%. Extension of zone 3 is not necessary in this case.

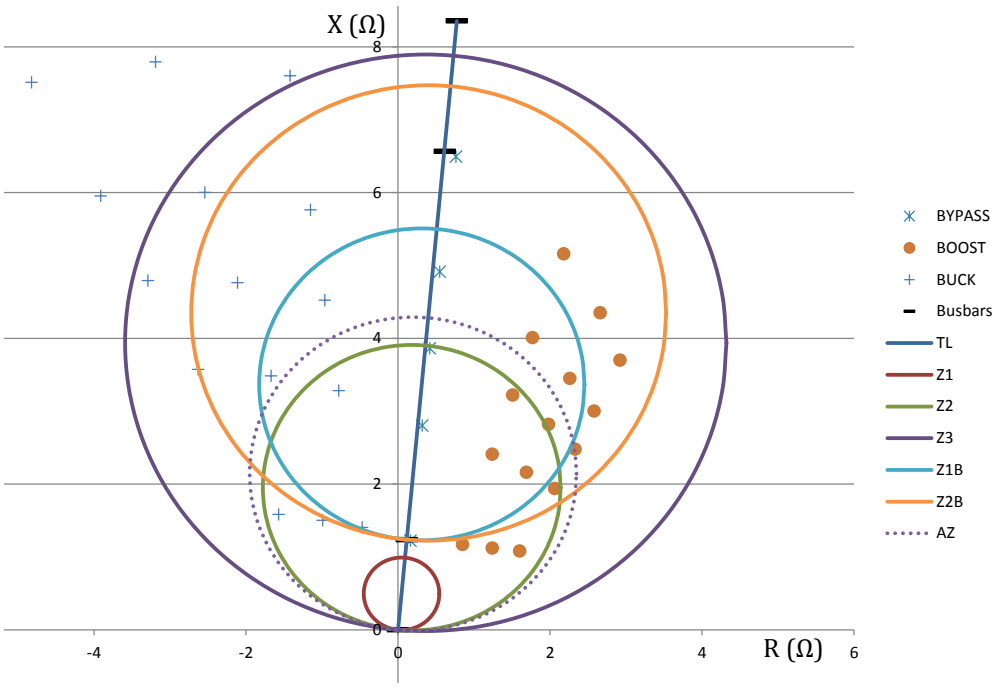

Figure 4-4 Mho diagram showing extended zone 2 (AZ) for QB boost mode

While the QB is in buck mode, zone 2 reach will need to be increased further. To fully compensate for the under reach, its reach will need to be extended to 7.6Ω as shown in Figure 4-5. The new reach results in mis-coordination with zone 2 of the adjacent circuit which is unacceptable. It also provides the same coverage as that of zone 3 which diminishes zone 2 purpose of remote back up while at the same time providing reasonable selectivity. The extent of the reach will need to be limited to a maximum of 180% to coincide with zone 1 reach of the adjacent line. This is depicted in Figure 4-6 and the resulting reach is 5.5Ω – an increase of 40.3%. Zone 3 is also extended by 44.1% to obtain a reach of 11.4Ω as shown in Figure 4-7. The obtained settings group are summarised in Table 4-1.

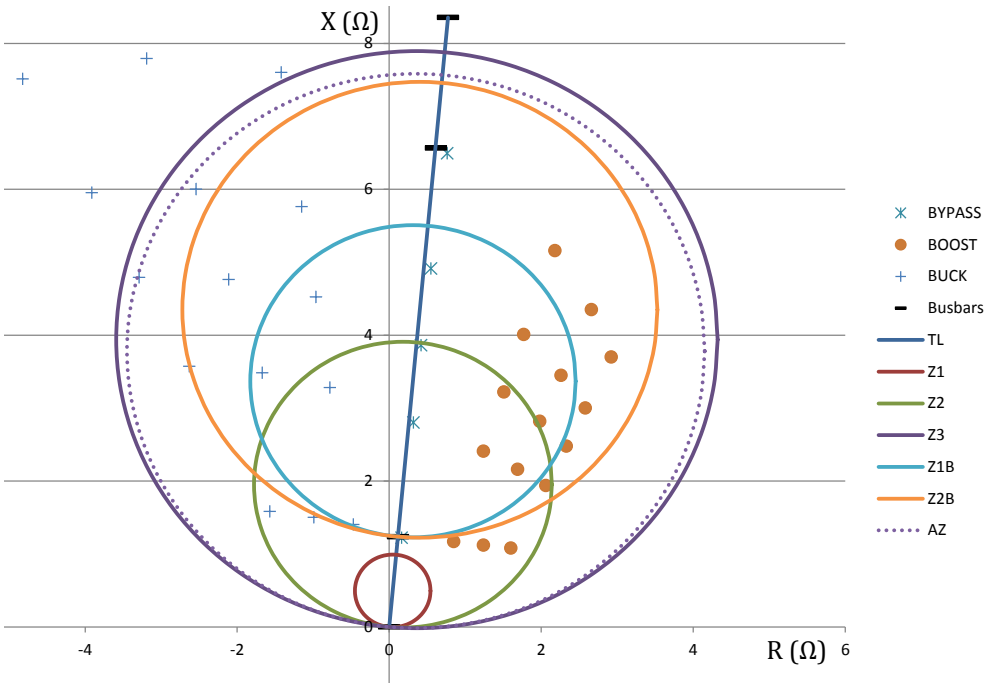

Figure 4-5 Mho diagram showing extended zone 2 (AZ) for QB buck mode to fully offset under reach issue

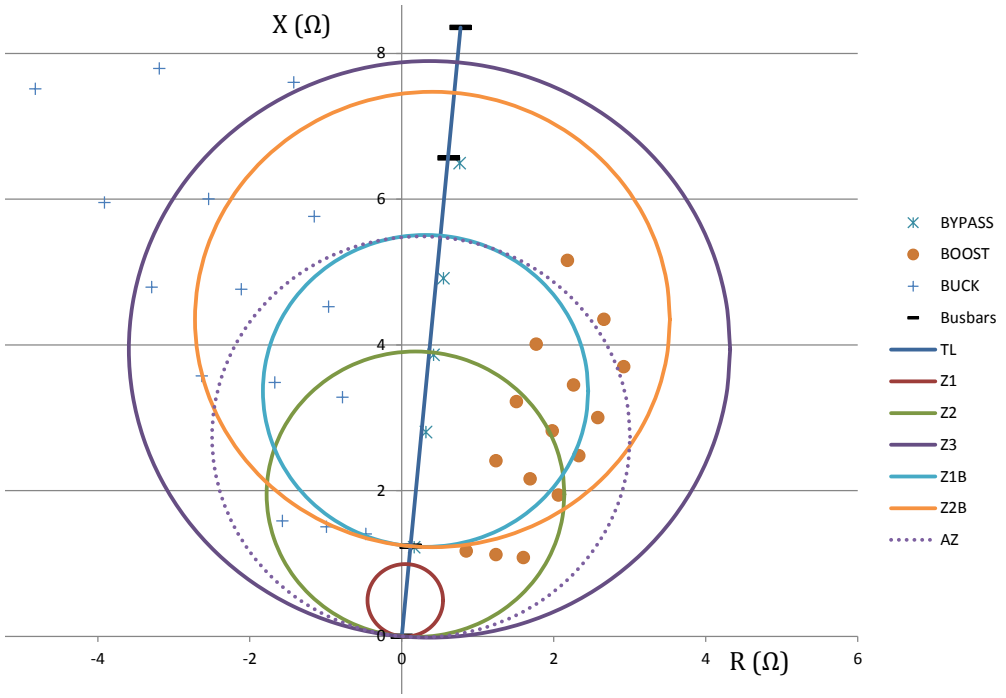

Figure 4-6 Mho diagram showing extended zone 2 (AZ) for QB buck mode to partially offset under reach issue

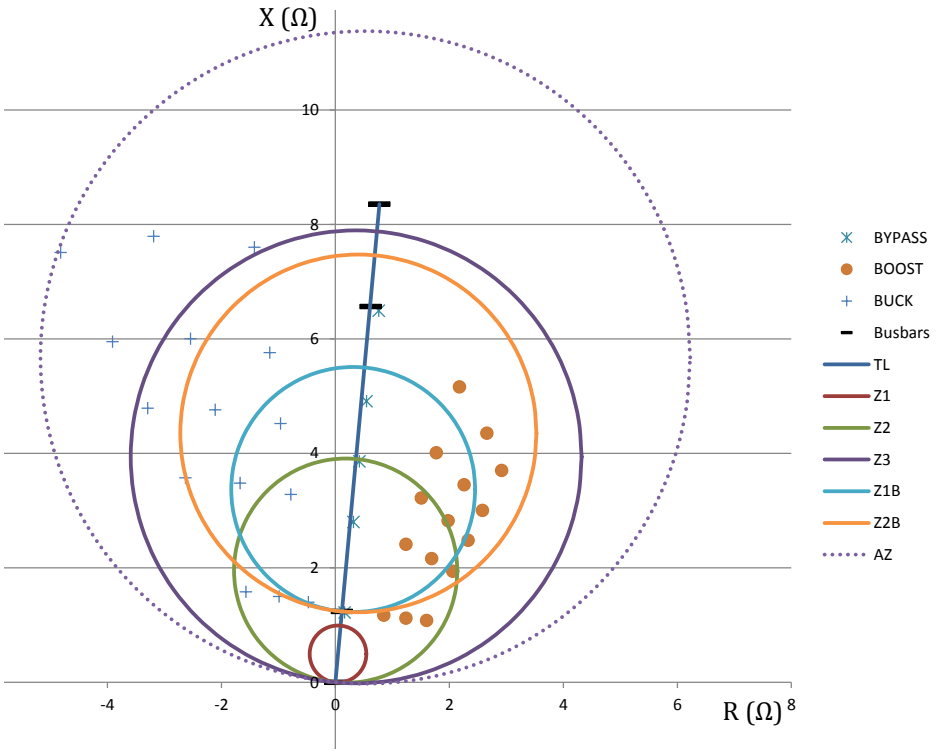

Figure 4-7 Mho diagram showing extended zone 3 (AZ) for QB buck mode

Table 4-1 Settings groups selected for the adaptive distance protection scheme

SG	Protection zone	Reach (Ω)	Reach increase (%)
1 (default)	Zone 1	0.994	-
	Zone 2	3.918	-
	Zone 3	7.663	-
2	Not used		
3	Zone 1	0.994	0
	Zone 2	4.3	9.7
	Zone 3	7.663	0
4	Zone 1	0.994	0
	Zone 2	5.5	40.3
	Zone 3	11.4	44.1

4.5.3 Settings group for a fall back situation

The adaptive settings selection logic is independent of the protection IED. This means that failure in the logic due to communications failure or otherwise may result in the activation of a settings group that is inappropriate for a given primary system condition. Therefore it is necessary to put in place a fall back mechanism which can be in the form of a default settings group that the IED reverts to when the communication with the adaptive logic is lost.

In this particular case, there are three options:

- Use the default reach settings group.
- Use the extended reach settings group.
- Use a dedicated settings group for the fall back situation.

Using the third option is not meaningful since the first two settings groups have been designed to cope with all envisaged primary system conditions (e.g. QB states). Therefore, a new settings group will not map to any of the states identified in the design stage. The second option can result in over reaching when the QB may be disengaged or short adjacent short circuits are energised. This is not preferred as loss of coordination is worse than a temporary under reach. The first option, as explained earlier, was selected by design to cope with situations where mis-coordination with adjacent short feeder and potential load encroachment are possible. These are the situations where protection mal-operation may occur when communication between the adaptive logic and the IED is lost. Therefore, the use of the default settings group as a fall back strategy is preferred.

A fail safe approach to implementing this fall back mechanisms can be achieved using the IED PSL. The PSL can be configured to revert to the default setting when communication failure is detected.

4.5.4 Settings group selection implementation with a physical relay

Figure 4-8 illustrates the implementation of the settings group selection mechanisms using a commercial protection relay (Alstom MiCOM P446 distance protection IED [27]). This IED offers four settings groups that can be activated through the programmable scheme logic (PSL). The two binary inputs SGx1 and SG1x are used for this purpose where the 'x1/1x' suffix denotes the active bit which determines the settings group to be activated as shown in Figure 4-8. To configure the PSL, Alstom MiCOM S1 Studio IED configuration tool was used [28].

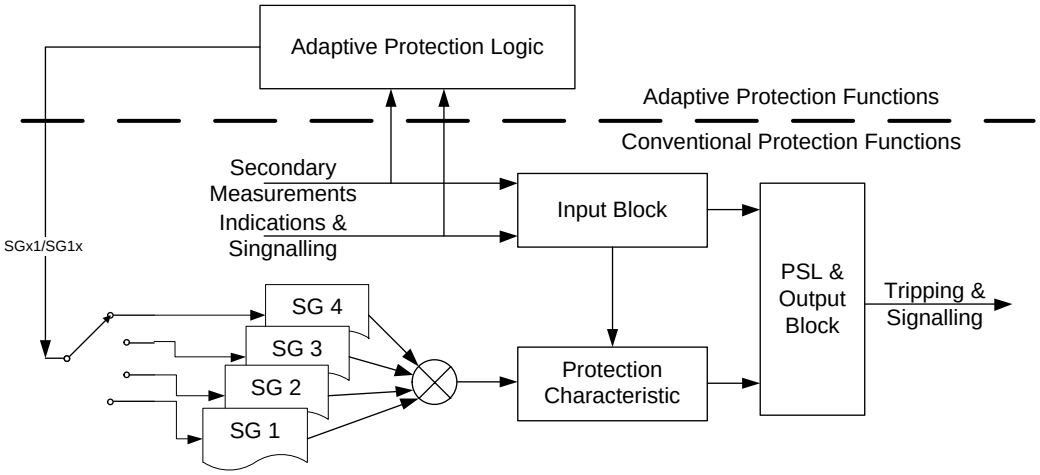

Figure 4-8 Settings group selection implementation

Table 4-2 Active settings groups using the relay binary inputs

Active Settings Group	SGx1	SG1x
SG1	0	0
SG2	1	0
SG3	0	1
SG4	1	1

The PSL specific to the settings group selection is shown in Figure 4-9. The PSL contains mappings of the physical binary inputs and the internal accessible variables – in this case SGx1 and SG1x. IED LEDs can also be configured for a visual indication of the active settings group. The adaptive logic requires knowledge of the active settings group for verification purposes. Details of the adaptive logic are left for the following chapter but are in line with the general setting selection strategy depicted in Figure 4-2.

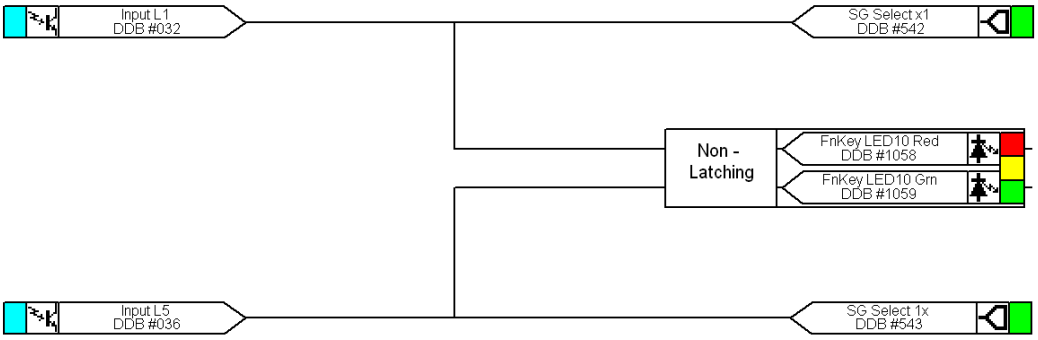

Figure 4-9 Alstom P446 PSL for settings group selection

If more settings groups are required than the relaying platform is capable of, then the settings group selection mechanism depicted in Figure 4-10 can be implemented. Implementing this method is out with the thesis scope and is for illustration purposes. The mechanism relies on storing the pre-calculated settings groups external to the relay. The adaptive logic would then select the appropriate settings group from the available pool and the chosen settings group parameters would then be written to the relay's active settings group.

The relay's proprietary communications protocols (in this case Courier protocol) can be used for the data exchange. However, settings group control mechanisms specified by IEC 61850 are preferred to achieve interoperability and replicate the configuration more easily. The adaptive logic requires an IEC 61850 MMS client implementation to communicate the settings group configuration commands [29]. On the relay end, an IEC 61850 MMS server is required to receive and process these commands using an IEC 61850 settings group control block (SGCB) [29]. In this case the selected settings group from

the available pool will simply be written to the active settings group in the relay using an IEC 61850 write service. For verification purposes, the active settings group parameters can be interrogated using an IEC 61850 read service. In addition to editing the active settings group, a settings group selection may also be implemented as a fall back mechanisms in the case of communications failure. The setup would require two settings groups in the IED. The first contains default parameters and cannot be remotely edited. The second settings group can be written to and remains active as long as the communications remains healthy. The SGCB can be configured to switch to the first settings group in case the communications fail. The rationale for using the default settings group as a fall back strategy has already been explained in section 4.5.2.

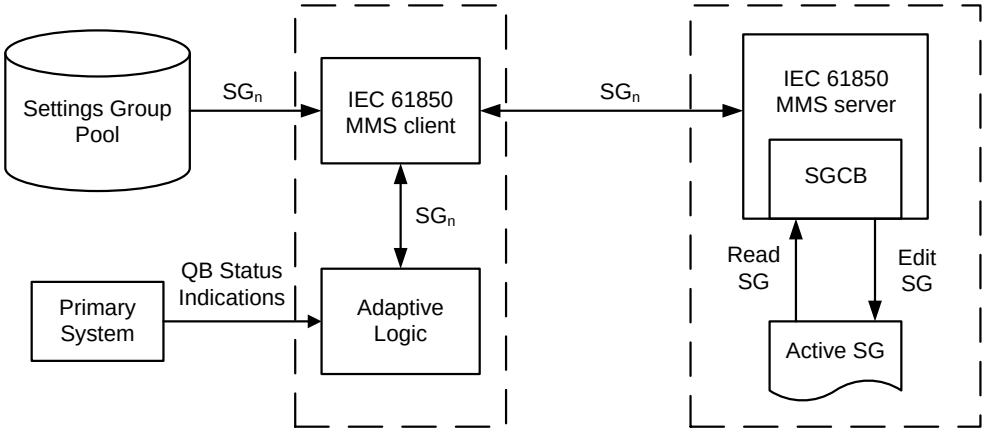

Figure 4-10 Using IEC 61850 for selecting between a large number of settings groups

4.6 Choosing the number of settings groups for adaptive protection

So far the number of settings groups was chosen based on two factors – the protection application and the platform capabilities. However, the latter should not pose a significant limitation in the number of possible settings groups with the aid of additional engineering effort (as shown in Figure 4-10). Having said that, additional bespoke functionality to increase the available number of settings groups increases the complexity of the solution and consequently verification requirements are increased. Therefore, a relaying platform with a larger number of settings groups is preferred.

Using a larger pool of settings groups increases the flexibility of the scheme by providing a finer resolution response for variable power system conditions. This, however, blurs the boundary between settings groups and online calculation of settings, thus diminishing the value of using settings groups in the first place. This coupled with the fact that it is unlikely for short circuit protection to experience an infinite number of power system variation that warrant a setting change with a marked improvement in performance.

The first factor, that is the application, can be reliably used to determine the maximum number of setting groups necessary. For the distance protection reach the international standard IEC 60255 [26] specifies that the MHO characteristic should exhibit at least +/-5% accuracy in terms of its reach. To this end, this can be used as a guideline to determine the realistic performance gains obtained from each additional settings group.

With reference to Table 4-1, SG 3 increases the reach by 9.7%. This means that a single settings group for this situation is sufficient. However, for SG4 a reach increase of 40.3 and 44.1% for zone 2 and zone 3 are achieved respectively (see Table 4-2). Based on the 5% accuracy discussed earlier, the maximum reach increase of 44.1% can be achieved with eight 5% reach increments. This translates into eight settings groups for this particular case study. As such a total of 10 settings groups can be used including SG1. The suggested 10 settings groups are summarised in Table 4-3. This shows the percentage increase of reach for each settings group relative to the default settings group SG 1. The associated accuracy range for each settings group is also given. Note that these settings groups are only for guidance purposes since the implementation (as shown in chapter 5) is limited to the 3 settings groups summarised in Table 4-1.

Table 4-3 Recommended number of settings groups indicating reach improvement

Settings group	Reach increase (%)	Accuracy range for increased reach (%)
SG 1 (default)	0	N/A
SG3	5	0-10
SG 4.1	5	0-10
SG 4.2	10	5-15
SG 4.3	15	10-20
SG 4.4	20	15-25
SG 4.5	25	20-30
SG 4.6	30	25-35
SG 4.7	35	30-40
SG 4.8	40	35-45

4.7 Chapter summary

Following on from the previous chapter's argument of the necessity to provide flexibility in protection functionality, this chapter examined the use of adaptive techniques to achieve this goal. This chapter reviewed the wealth of literature available on the subject while limiting the scope to schemes that address protection performance issues of sensitivity or coordination. The adaptive techniques proposed in the literature varied in terms of performance advantages, implementation complexity and speed of operation. However, no particular technique stood out as being favourable.

The chapter did not attempt to address deficiencies in proposed adaptive protection techniques. Alternatively, it focussed on identifying problems associated with their applicability in a real power system. To this end a number of technical and institutional challenges to adopting the adaptive protection philosophy were defined.

With the aid of common definitions of adaptive protection, the scope of its use or deployment has been defined. Adaptive protection schemes are argued to be best suited for enhancing the performance of conventional protection schemes in response to pre-fault events such as topology changes or FACTS device mode changes.

The adaptive protection approach adopted by this chapter relied on the use of three settings groups that can be dynamically activated to enhance the performance of the distance protection scheme in question. The example provided was based on the case study presented in the previous chapter. A general strategy for an adaptive settings group selection was presented which relies on measuring the state of the QB in the studied circuit. Strategies to cope with potential mis-coordination, load encroachment and communications failure were also presented. The chapter also proposed an implementation based on IEC 61850 to enable the use of more settings groups than the relating platform of choice can offer.

4.8 References

[1] T. E. Dy Liacco, "The Adaptive Reliability Control System," *Power Apparatus and Systems, IEEE Transactions on,* vol. PAS-86, pp. 517-531, 1967.

[2] IEEE, "IEEE Std C37.113-1999: IEEE Guide for Protective Relay Applications to Transmission Lines," ed, 2000.

[3] R. K. Aggarwal, A. T. Johns, Y. H. Song, R. W. Dunn, and D. S. Fitton, "Neural-network based adaptive single-pole autoreclosure technique for EHV transmission systems," *Generation, Transmission and Distribution, IEE Proceedings-,* vol. 141, pp. 155-160, 1994.

[4] S. P. Le Blond and R. Aggarwal, "Design of Adaptive Autoreclosure Schemes for 132 kV With High Penetration of Wind—Part II: Real-Time Development and Testing," *IEEE Transactions on Power Delivery,* vol. PP, pp. 1-1.

[5] S. Bruno, M. De Benedictis, M. La Scala, S. Lamonaca, G. Rotondo, and U. Stecchi, "Adaptive relaying to balance protection dependability with power system security," in *Computational Technologies in Electrical and Electronics Engineering (SIBIRCON), 2010 IEEE Region 8 International Conference on*, 2010, pp. 482-487.

[6] A. Y. Abdelaziz, H. E. A. Talaat, A. I. Nosseir, and A. A. Hajjar, "An adaptive protection scheme for optimal coordination of overcurrent relays," *Electric Power Systems Research,* vol. 61, pp. 1-9, 2002.

[7] M. Sanaye-Pasand and P. Jafarian, "An Adaptive Decision Logic to Enhance Distance Protection of Transmission Lines," *IEEE Transactions on Power Delivery,* vol. 26, pp. 2134-2144, 2011.
[8] Y. Zhu, S. Song, and D. Wang, "Multiagents-based wide area protection with best-effort adaptive strategy," *International Journal of Electrical Power & Energy Systems,* vol. 31, pp. 94-99, 2009.
[9] J. C. Tan, P. A. Crossley, D. Kirschen, J. Goody, and J. A. Downes, "An expert system for the back-up protection of a transmission network," *IEEE Transactions on Power Delivery,* vol. 15, pp. 508-514, 2000.
[10] S. M. Brahma and A. A. Girgis, "Development of Adaptive Protection Scheme for Distribution Systems With High Penetration of Distributed Generation," *IEEE Transactions on Power Delivery,* vol. 19, pp. 56-63, 2004.
[11] M. Jin and T. S. Sidhu, "Adaptive load encroachment prevention scheme for distance protection," *Electric Power Systems Research,* vol. 78, pp. 1693-1700, 2008.
[12] A. Saffarian and M. Sanaye-Pasand, "Enhancement of Power System Stability Using Adaptive Combinational Load Shedding Methods," *Power Systems, IEEE Transactions on,* vol. PP, pp. 1-11, 2010.
[13] J. C. Tan, P. A. Crossley, and P. G. McLaren, "Fuzzy expert system for on-line fault diagnosis on a transmission network," in *IEEE Power Engineering Society Winter Meeting, 2001*, 2001, pp. 775-780 vol.2.
[14] N. G. Chothani, B. R. Bhalja, and U. B. Parikh, "New fault zone identification scheme for busbar using support vector machine," *Generation, Transmission & Distribution, IET,* vol. 5, pp. 1073-1079, 2011.
[15] T. S. Sidhu, D. S. Baltazar, R. M. Palomino, and M. S. Sachdev, "A new approach for calculating zone-2 setting of distance relays and its use in an adaptive protection system," *Power Delivery, IEEE Transactions on,* vol. 19, pp. 70-77, 2004.
[16] M. Sanaye-Pasand and P. Jafarian, "Adaptive Protection of Parallel Transmission Lines Using Combined Cross-Differential and Impedance-Based Techniques," *IEEE Transactions on Power Delivery,* vol. 26, pp. 1829-1840, 2011.
[17] K. El-Arroudi and G. Joos, "Data Mining Approach to Threshold Settings of Islanding Relays in Distributed Generation," *Power Systems, IEEE Transactions on,* vol. 22, pp. 1112-1119, 2007.
[18] H. Shyh-Jier and L. Jeu-Min, "Enhancement of anomalous data mining in power system predicting-aided state estimation," *Power Systems, IEEE Transactions on,* vol. 19, pp. 610-619, 2004.
[19] E. E. Bernabeu, J. S. Thorp, and V. Centeno, "Methodology for a Security/Dependability Adaptive Protection Scheme Based on Data Mining," *IEEE Transactions on Power Delivery,* vol. PP, pp. 1-1.
[20] M. M. Mansour, S. F. Mekhamer, and N. E. S. El-Kharbawe, "A Modified Particle Swarm Optimizer for the Coordination of Directional Overcurrent Relays," *IEEE Transactions on Power Delivery,* vol. 22, pp. 1400-1410, 2007.

[21] H. Ying-Yi and C. Po-Hsuang, "Genetic-Based Underfrequency Load Shedding in a Stand-Alone Power System Considering Fuzzy Loads," *IEEE Transactions on Power Delivery,* vol. 27, pp. 87-95, 2012.
[22] H. Seyedi and M. Sanaye-Pasand, "New centralised adaptive load-shedding algorithms to mitigate power system blackouts," *Generation, Transmission Distribution, IET,* vol. 3, pp. 99-114, 2009.
[23] N. Schaefer, T. Degner, A. Shustov, T. Keil, and J. Jaeger, "Adaptive protection system for distribution networks with distributed energy resources," in *Managing the Change, 10th IET International Conference on Developments in Power System Protection (DPSP 2010)*, 2010, pp. 1-5.
[24] A. Apostolov, "Multi-agent systems and IEC 61850," in *Power Engineering Society General Meeting, 2006. IEEE*, 2006, pp. 6-pp.
[25] W. Hui, K. K. Li, and K. P. Wong, "An Adaptive Multiagent Approach to Protection Relay Coordination With Distributed Generators in Industrial Power Distribution System," *Industry Applications, IEEE Transactions on,* vol. 46, pp. 2118-2124, 2010.
[26] IEC, "IEC 60255: Measuring relays and protection equipment," ed, 2010.
[27] Alstom, *Network Protection and Automation Guide - Protective Relays, Measurement and Control*, 2011.
[28] Alstom, *MiCOM P341 Interconnection Protection Relay Technical Manual*: Alstom Grid, 2011.
[29] IEC, "IEC 61850: Communication networks and systems in substations," ed, 2003.

5 Requirements specification, architectural design and overall validation of adaptive protection schemes

5.1 Chapter methodology and contributions

It is necessary to shift some of the emphasis of adaptive protection scheme development from algorithm focused design to system based design. This facilitates improved integration of such schemes into digital substations as well as the application of more effective testing strategies based on traceable requirements. This underlying hypothesis will be tested through the design and implementation of the adaptive distance protection scheme proposed in the previous chapter. In doing so, the following main chapter contributions will be made:

- Demonstration of the effectiveness of the proposed adaptive distance protection scheme under varied QB operating conditions while utilising multiple settings groups.
- Unique application of systems engineering based specification, design, implementation and validation to adaptive protection schemes. This takes into account the lifecycle requirements associated with the scheme. This process is seen to be essential if adaptive protection is to be considered as a viable and practical solution.
- Identification of the shortcomings of simulation based validation of adaptive protection schemes. Such limitations stem from test case definitions.

5.2 Overview of adaptive protection design and architectures

As discussed in chapter 4, there are numerous examples of adaptive protection schemes which demonstrate their ability to deal with flexible network operation with varying degrees of success. However, up until recently, no reported efforts have been made to formally define and design the functions constituting an adaptive protection scheme, nor the interaction between such schemes and the surrounding operating environment (e.g. substation environment including automation functions). These are important matters that should be taken into consideration as will be discussed and demonstrated in the remainder of the chapter.

Architectural design of adaptive protection is one of the focal points of this work. The adaptive protection architecture (APA) developed here was first proposed by Tumilty in [1]. This presented an 'implementation architecture' which facilitates the mapping between function of the scheme and the physical elements (or devices) that constitute the scheme. This abstraction is achieved in a similar fashion to that used by communications architectures that separate data objects from low level protocols, but use mappings between these to achieve the required functionality in a more flexible manner. The architecture assumes three functionally abstract layers as shown in Figure 5-1.

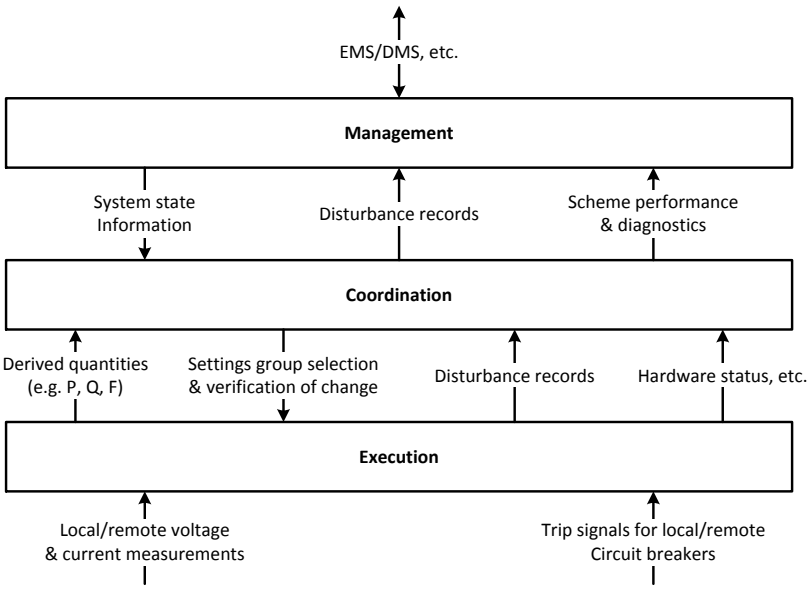

Figure 5-1 Original proposed adaptive protection architecture [1]

The functionality that each layer represents can be summarised as follows:

- Execution layer: this constitutes the conventional protection functions that execute well established algorithms to detect and isolate faults in typically under a second.
- Coordination layer: this layer maps settings groups used by the execution layer to the power system state. It then activates new settings group when necessary and verifies that the activation has been successful.
- Management layer: this layer interacts with the energy/distribution management system (EMS/DMS) to provide system wide information of relevance to the adaptive protection scheme. Such information includes blocking protection operation under certain disturbances if protection operation is deemed detrimental to the performance of the power system. Such blocking signals usually only operate with non-short circuit type protection (e.g. frequency protection).

The work in this thesis develops the APA further to address the following two main issues in the original treatment of the APA:

- Conceptual applications for the APA were proposed for a distribution network application related to frequency protection and islanding. Therefore it is not clear if it is applicable to a transmission protection application or indeed a wide area based protection scheme. This is because the presentation of the APA was mostly implementation driven, which although aiding the understanding of the APA, can limit the appreciation of its usefulness to other applications.
- The boundaries of coordination and management layers were not clearly defined in terms of constituent functions, minimum interfaces and extent of authority. Furthermore, the approach to the adaptation of protection was limited to settings group changes, which does not accommodate other potentially viable approaches.

The treatment of the APA in this chapter will therefore address the above issues with the aid of the developed adaptive distance protection scheme. Specifics will be examined in the following sections.

5.3 Adaptive protection lifecycle requirements

Similar to any engineering system, adaptive protection schemes undergo a series of lifecycle stages, each of which dictate a unique yet highly interdependent set of requirements. These life cycle stages are scheme design and implementation, scheme installation and commissioning, scheme operation and maintenance and finally scheme decommissioning and replacement. The requirements for each stage are developed in the following section based on standard systems engineering approaches [2]. It is first necessary to distinguish between the different types of requirements and how these apply to adaptive protection schemes.

The process of determining the scheme requirements starts with the elicitation of the user (system operator) requirements [2]. This reflects the expectations of the scheme user and these are mainly driven by their protection policy. One of the main barriers to the adoption of an adaptive protection philosophy is an institutional one and is manifested by the inadequacy of utility policy in accommodating such functionality. Consequently, determining the related user requirements is one of the first steps in embracing the adaptive protection philosophy. It is imperative that the additional functionality offered by adaptive protection does not cause degradation in scheme performance. The consequences of additional complexity in scheme implementation as a result of added flexibility in operation must be understood. De-risking these consequences can be managed by adopting effective testing strategies and ensuring that the user requirements are always taken into account during scheme development. A subsequent set of system requirements are devised accordingly taking the form of non-functional, functional and performance requirements as shown in Figure 5-2 [2]. Non-functional requirements refer to aspects such as the reliability of the scheme [3], redundancy measures and compliance with EMC (electromagnetic compatibility) specifications. Non-

functional requirements considered in this chapter in relation to adaptive protection are related to the layout and relationship between the constituent elements of the scheme.

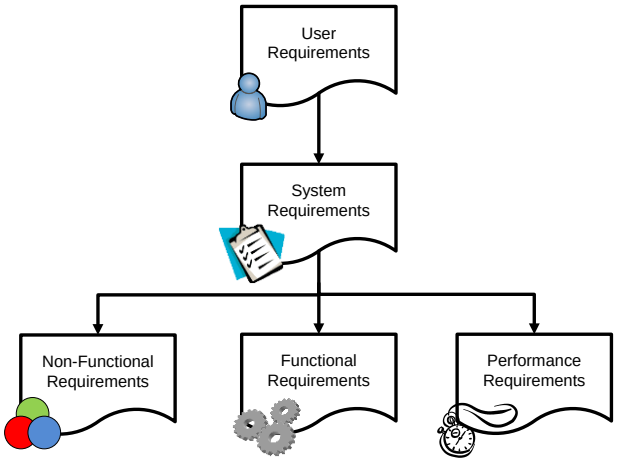

Figure 5-2 Development of requirements for a system

Minimum functionality required by an adaptive protection scheme will be detailed in the APA developed in section 5.4. This will specify the interfaces and interactions between the constituent functions. Some of the minimum functionality must be qualified in terms of performance. For example, the accuracy by which a reach error is determined or the frequency and timeliness of executing a specific function. The performance in terms of delivering protection functionality (i.e. reliable fault detection and clearance) will be based on a fundamental requirement – that is the performance expected of existing protection schemes in terms of speed, selectivity and stability shall not be compromised or degraded by the introduction of adaptive functionality.

The requirements associated with each lifecycle stage of adaptive protection are specified in the following subsection. It is important to note that these do not serve as a detailed requirements specification document, but this treatment aims to pick out the requirements that are most relevant to adaptive protection functionality, and as such were not specified elsewhere in the literature. These will then play an important part in developing the adaptive protection architecture in section 5.4. Finally these requirements will be revisited in the scheme design, implementation and testing sections 5.5-5.6.

5.3.1 Scheme design and implementation requirements

The introduction of adaptive protection functions into substations should take into account existing protection arrangements that will coexist with adaptive protection functionality. This should also consider methods to integrate such functions into existing substations with full view of future digital substations. Practically, these considerations entail the following requirements:

- Adaptive functions should support existing data exchange mechanisms in a substation while being able to accommodate future mechanisms for data exchange in light of emerging standards (e.g. IEC 61850 [4]).
- Adaptive protection functions should capitalise on existing and established protection functions if these functions provide an effective route through which adaptive functionality improves the performance of these functions.
- Adaptive protection functionality should only be sanctioned when the performance of the existing conventional 'static' protection functions does not meet performance requirements specified by the scheme user.
- The process of designing adaptive protection functionality should ensure requirements traceability to facilitate the process of verification and validation of the adaptive protection functions and scheme.

The requirements above emphasise the necessity of minimising disruption to existing protection functions both during integration into the substation and during scheme operation. The capabilities of the scheme will always be bound by the hardware and software implementation limitations. This is perhaps less of an issue with modern computing platforms and new generation IEDs from a performance point of view. Having said that, it is necessary to recognise which of the requirements should be platform independent and which should be constrained closer to the implementation phase. For instance, adopting an IEC 61850 data model should be independent of the platform of choice. In fact, this requirement should dictate the platform specification. However, realising transient based protection functions requires a mature gigabit Ethernet solution at the IED end, which is a platform and standardisation limitation [5].

5.3.2 Scheme installation and commissioning requirements

Requirements for installing an adaptive protection scheme draw heavily from the design and implementation requirements, especially those related to the integration within a substation. However, one of the most significant challenges associated with this lifecycle stage, is the site commissioning tests (SCT) conducted on the scheme after installation. These ensure that the scheme is installed correctly and functions perform as specified during tests. As such the following requirements can be specified:

- Adaptive protection schemes shall provide an SCT mode where tripping commands and other interaction with the rest of the substation are logically disabled to avoid causing a mal operation. Furthermore, the adaptive functions shall also identify input signals which are specified as test inputs which do not warrant a reaction from the adaptive scheme. To minimise the requirement for substation outages, an SCT mode can operate in parallel with the normal scheme operation without affecting the scheme performance or as shown in Figure 5-3.
- A new generation of toolsets are required to generate and monitor virtual (i.e. LAN based) test signals according to a predefined set of commissioning tests. These tests shall be designed to verify general adaptive protection functionality such as settings changes as well as scheme specific functionality (e.g. performance evaluation of distance protection reach).

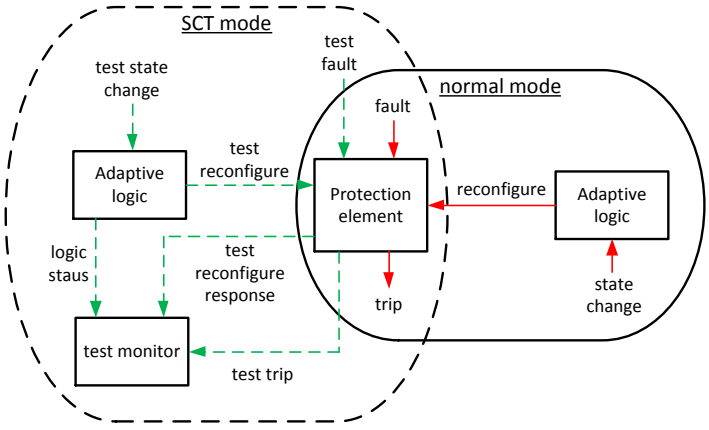

Figure 5-3 Behaviour of adaptive scheme under SCT and normal operating modes

5.3.3 Scheme operation and maintenance requirements

Settings management plays an important role in the operation of adaptive protection schemes. Although adaptive schemes by definition alter their settings or configuration to deal with changes in the power system, ensuring that the mechanism through which these settings are altered remains fit for purpose is important. Protection diagnostics are critical to the effective operation of and maintenance of protection schemes in general. This is no different with adaptive protection. However, the process of fault reporting and subsequent diagnostics should take into account the additional capabilities offered by the adaptive and supporting functions. Both these aspects require performing self-verification at different functional levels of the scheme. As such the following is required:

- The adaptive protection scheme shall perform a self-verification function which aims to identify performance shortfalls in the scheme for a given power system condition and trigger an adaptation accordingly. The aim of the adaptation is to align the performance of the scheme at any given time with that specified by the system operator.
- Regular high level reporting of scheme performance shall be conducted by passing self-verification function outputs to the system operator for ongoing diagnostics and refinement of the scheme where necessary. The high level reporting is performed to ensure that the adaptation does not have adverse effects on the system level (in addition to circuit level).
- The adaptive protection functions shall allow modification to the scheme to be conducted online by means of software/firmware upgrades. This cannot disrupt the operation of the scheme nor result in degraded performance over this upgrade period.

One of the key operational features of an adaptive protection scheme in this lifecycle stage is possessing self-verification functions. This means that the built-in functionality is capable of identifying instances of degraded performance and act upon them either by reporting these incidents to the operator (by means of an alarm) or by altering the scheme settings as determined by the design of the scheme. This can be thought of as an advanced ‘watchdog’ functionality with

corrective measures that seek to improve the performance of the adaptive scheme and/or seek operator intervention.

The level to which some of this functionality can be delivered is dependent on the capability of the adaptive protection platform. The number of tasks performed such as the self-verification, reporting, test signal handling (in SCT mode) may warrant a co-processor to handle these functions while freeing the main platform processor capacity to perform more time-critical protection functions. Alternatively, these functions can be deployed on a separate platform where data is exchanged between platforms as necessary over a communications network. In any case, this should not be taken as a guideline for the number of physical 'boxes' required. On the contrary, the adaptive functions should be platform agnostic and only implementation constraints should dictate specific deployment platform requirements.

5.3.4 Scheme decommissioning and replacement requirements

Requirements are refined continuously for adaptive protection schemes in light of their performance in the previous lifecycle stage. Moreover, evolving power system operating conditions may dictate that new functions should be added. Similar to the requirements associated with scheme maintenance, scheme replacement should not necessarily require physical replacement of associated secondary equipment. Software/firmware upgrades should be possible to minimise interruption and performance degradation of the scheme. The duration of the secondary system's operational lifecycle is much shorter than that of primary system equipment (typically 15 and 40 years respectively). As such it is necessary to put in place suitable interfaces between these systems to facilitate the replacement process.

5.3.5 Validation vs. verification of adaptive protection schemes

According to the IEEE standard for systems and software verification and validation (IEEE std. 1012-2012 [6]), the processes of verification and validation (V&V) involve the following:

- Verification provides objective evidence for whether a system satisfies the following:
  - Conforms to requirements during each life cycle stage.
  - Satisfies the relevant standards, practices and conventions during each lifecycle stage.
  - Successfully completes each lifecycle stage and satisfies the criteria for initiating a subsequent life cycle stage
- While validation provides objective evidence for whether a system satisfies the following:
  - Satisfies system requirements at the end of each life cycle stage.
  - Solves the right problem by correctly modelling and implementing the laws, rules and assumptions of problem or application domain.
  - Satisfies the intended use and user needs in the operational environment.

Verification is commonly referred to as 'building the thing right' and validation is 'building the right thing'. The V&V during the design and implementation lifecycle stage is usually represented using a V-Model as shown in Figure 5-4 [2, 7]. Each phase of development requires a specifically designed test to verify that outcomes of the stage comply with specifications. At the end of the development lifecycle stage, a complete system validation is performed to provide the objective evidence required as mentioned above.

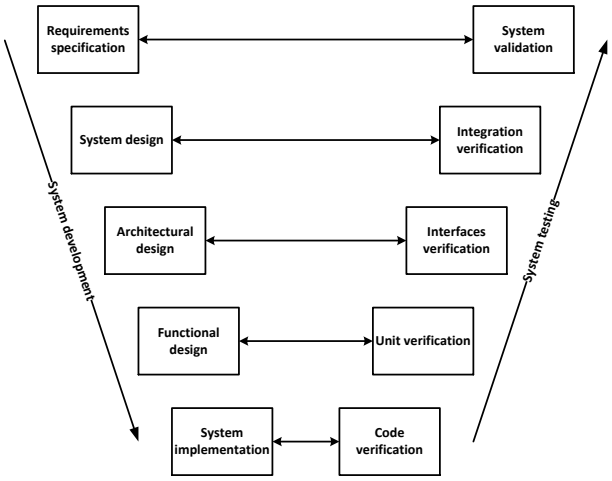

Figure 5-4 V-Model for the V&V of a system's design and implementation

But what does V&V mean for adaptive protection schemes and how can these processes be applied effectively? By taking the adaptive distance protection as an example, the process of verification must encompass all the constituent elements of the scheme. The distance protection elements for instance must comply with requirements specified by standards such as IEC 60255 [8]. Verifying the performance of the adaptive functions responsible for changing the active settings, however, is not as straightforward. In other words, no standard methods or policies provide guidance to achieving their verification. These questions are addressed in section 5.7 and in chapter 6.

5.4 Development of a detailed adaptive protection architecture

As mentioned earlier, the concept of an adaptive protection architecture (APA) was first proposed in [1]. To test the validity of the APA for the transmission protection application in this thesis and to determine its general applicability, it is necessary to achieve the following [9]:

- Define the functions that each of the architecture's layers perform.
- Define the breadth of influence that a higher functional layer of the architecture has on functions belonging to a lower layer.
- Determine the nature, frequency and timeliness of information exchanged between the architecture's layers.

For reference the APA developed in this thesis is shown in Figure 5-5 and each of its constituent elements is discussed in the following subsections.

5.4.1 The role of execution layer functions

As mentioned earlier, execution layer functions constitute conventional protection elements such as distance, over current and frequency protection relays. These react to faults or disturbances in the usual manner and their response time usually takes under 1s but more typically tens of milliseconds especially at the transmission level.

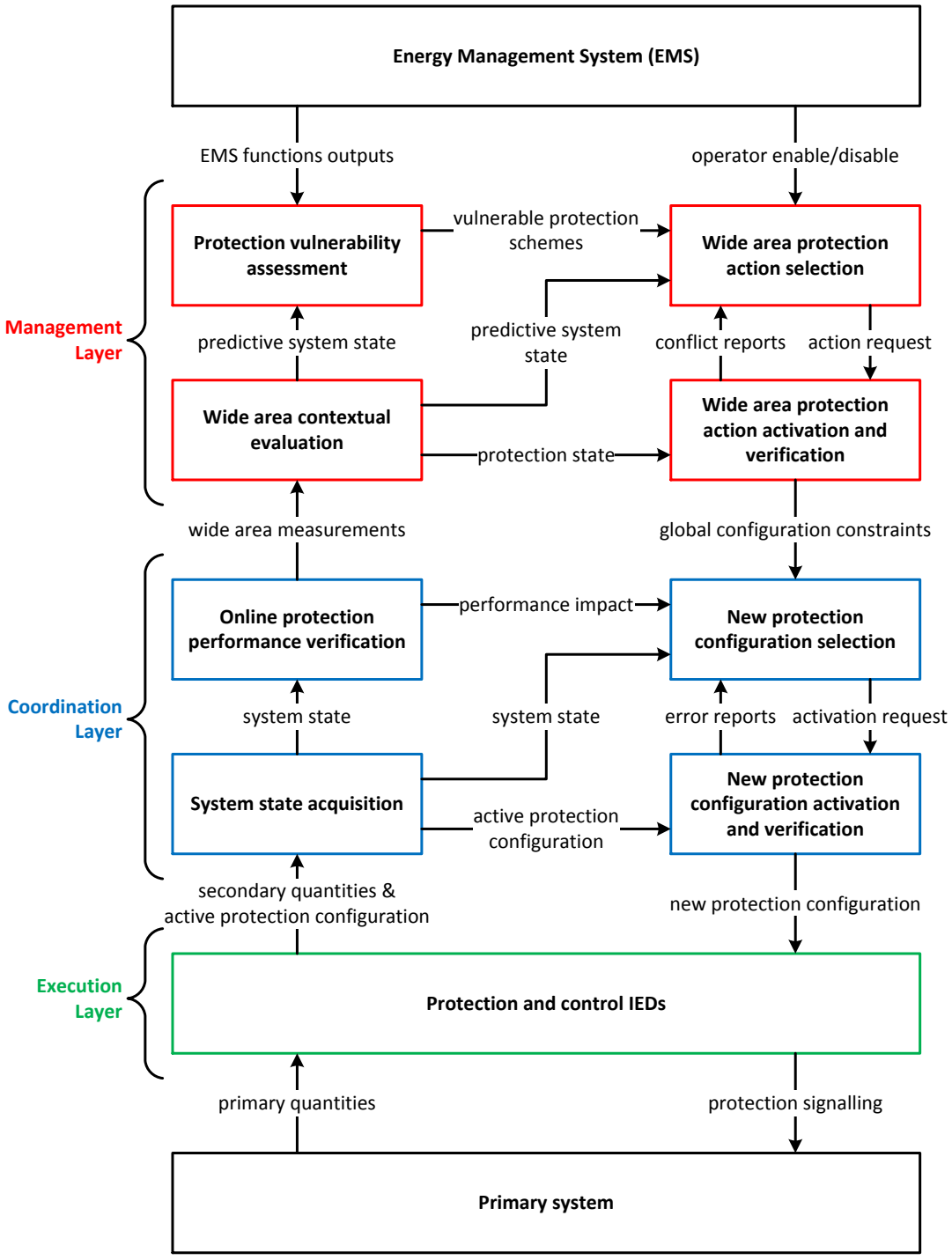

Figure 5-5 Developed adaptive protection architecture

As discussed before the adaptation of execution layer behaviour can be achieved through settings changes sanctioned by the coordination layer. However, as discussed in chapter 4, the role of adaptation through this method is restricted to pre-fault conditions where prevailing network conditions (or configuration) lead to the selection of a settings group better attuned to such conditions. The

draw back in this approach is that it is difficult to correct for protection performance shortfall that only manifest themselves during transients (e.g. current and voltage inversion effects in the presence of series compensation [10]). This role can be filled by more advanced transient based protection functions [11]. The implementation of such functionality is out with the scope of this thesis. However, to maintain the logical hierarchy of the APA it is necessary that any kind of protection functions operating at the execution level possess a degree of configurability (through settings or otherwise) to ensure flexibility in performance that can be fine tuned by the upper layers of the APA.

5.4.1.1 Scope and time response of the execution layer

The scope of the execution layer functions is defined by the scope of the scheme which is usually of a local nature. Only communications based protection schemes that incorporate protection signalling extend beyond the local scope of this layer. The execution layer has no direct influence on the operation of the upper APA functions, as their performance is purely based on the information reported by this layer.

The time response of these functions is defined by the application. Normally, faster operation (tens of milliseconds) is associated with transmission level protection. Distribution level short circuit protection may take just over a second to operate in extreme cases. In such cases, there is actually room for adaptive protection functionality to better optimise such occurrences for faster operation.

5.4.1.2 Execution layer interfaces

A minimum logical interface is defined to not restrict implementation options and at the same time ensure consistency between different implementations. The inputs to the layer are:

- Measurements from instrumentation sources for achieving specific protection functionality in addition to remote and local protection signalling (e.g. inter trip and breaker status respectively).

- A configuration change command, which can take the form of either a settings group selection or a direct settings write operation. This is triggered by the coordination layer and its frequency depends entirely on the frequency of changes in the network that warrant a change in settings. The configuration change can be extended to a change in scheme logic (PSL), but as discussed in the chapter 4, no evidence exists as to how this can be useful.

5.4.2 The role of coordination layer functions

The response of coordination layer functions is limited to pre-fault events. That is changes in the network conditions that warrant a change in execution layer configuration. To ensure that a change in network conditions is reflected accordingly in a new protection IED configuration, four functions are required:

- System state acquisition: the nature of information generated by this function takes the form of a status indication. This does not mean that this information is restricted to circuit breaker or tap changer position. In fact other types of information can be incorporated in this way such as the level of DG penetration reaching a predetermined critical level.
- Online protection performance verification: The expected and actual performance of the execution layer functions based on system conditions is performed here. System status information generated by the previous functions is utilised.
- New protection configuration selection: Whether settings are calculated on the fly or selected from a predetermined pool of settings groups, the associated logic selects the most appropriate setting to minimise the performance shortfall (e.g. reach error) reported by the performance verification function.
- New protection configuration activation and verification: this function deals with low level communications to activate the new protection configuration. Once the activation is performed, it is verified by interrogating the status of the execution layer IEDs.

5.4.2.1 Scope and time response of the coordination layer

Since coordination layer functions operate directly on execution layer functions, their scope of actions does not go beyond that of the execution layer's protection scheme. The scope of the information required by its functions is determined by offline studies that quantify the impact of different network conditions on the scheme (short of wide area disturbances). The time frames involved from condition changes to settings changes can take up to a few seconds depending on the type of performance verification conducted.

5.4.2.2 Coordination layer interfaces

One of the important issues that need to be taken into account is the timeliness of the configuration changes sanctioned by the coordination layer. An acceptable finite amount of time required for these changes in governed by:

- The likelihood of a fault or disturbance occurring this time.
- The criticality of the protected network and the impact that leaving the network in a degraded protection state has on this network.

5.4.3 The role of management layer functions

The goals of verifying protection performance and initiating adaptive configuration of protection are echoed in the management layer. But this is where similarities with the coordination layer end as this layer has a wider system scope and different emphasis in operating time scales and performance improvement objectives.

In the case of the coordination layer, the impact on scheme performance is evaluated at the scheme level and can be potentially implemented for all protection schemes. However, the evaluation of system wide information for protection purposes during wide area disturbances is less feasible at the scheme level. Therefore, it is necessary to rely on wide area measurements to achieve this evaluation. This is then followed by identifying the protection schemes that are most vulnerable to these disturbances and adapt their configuration accordingly. Protection vulnerability has been discussed in literature as a means of identifying relays which are most likely to mal-operate under stressed

conditions due to load encroachment for instance. A number of indices have been proposed to quantify such vulnerability [12-14]. By employing a similar approach, the response of the management layer can be more targeted and no fixed associations with protection scheme are required. The functions constituting the management layer generally operate in the same way their counterparts in the coordination layer do. This in essence identifies the potential performance shortfalls in protection and reacts by issuing corrective measures.

5.4.3.1 Scope and time response of the management layer

The nature of protection issues that the management layer deals which lends itself to close integration with system integrity protection schemes (SIPS) [15]. Consequently the management layer requires information produced by the system operator (EMS, energy management system) to identify stressed power system conditions and how these conditions are evolving over time in different parts of the system. The nature of power system phenomena dictates the response time frames of the management layer which can be in the order of several seconds or even minutes when dealing with slow stability issues (e.g. voltage instability) and the potential for cascade tripping. This brings forward a requirement to possess predictive protection impact capabilities not too dissimilar to predictive out of step functionality [7].

The management layer will have a more varied set of options when issuing an adaptive protection action depending on the developing power system situation. Actions can range between scheme blocking signals to defining maximum and minimum boundaries for the possible settings options selected by the coordination layer. When several actions are possible, then these can be ranked in terms of their effectiveness in achieving increased protection security or dependability before issuing the appropriate command [16].

5.4.3.2 Management layer interfaces

While the management layer has significant interactions with the system operator (EMS), it does not necessarily need to physically reside in a control

room. Access to the required information is what counts. The minimum information necessary is obtained from wide area measurements, state estimation functions and manual operator overrides.

5.5 Design and implementation of the proposed adaptive distance protection scheme

In chapter 4, the algorithm for the proposed adaptive distance protection scheme was presented in Figure 4-2. The flowchart focuses on the processes associated with identifying distance reach errors due to different primary system triggers. This section will present how this core functionality is realised in line with the APA functional layers. From the outset, the required functionality is organised to reflect the APA layers and as such the following subsections will discuss the associated functions individually.

The distance protection algorithm was implemented in Simulink for subsequent deployment in a substation computer (PC target). This choice was influenced by the following [17]:

- The ability to generate code and deploy the algorithm on a variety of targets (embedded or otherwise). This is critical for a model based design methodology which facilitates the verification and validation of developed algorithms. Furthermore, errors introduced by the user are minimised during the automatic code generation.
- Potential for integrating advanced Simulink functionality such as additional component libraries, model checking, code optimisations and hardware in the loop capabilities.

Only coordination and limited management layer functionality are implemented in Simulink. Execution layer functionality is provided by a physical distance protection IED. The distinction between prototype and field adaptive scheme in terms of implementation decisions is discussed in 5.6.3. Figure 5-6 shows the structure of the Simulink model and how it interacts with the other elements of the scheme under different testing stages. The full Simulink model is presented in Appendix B for reference.

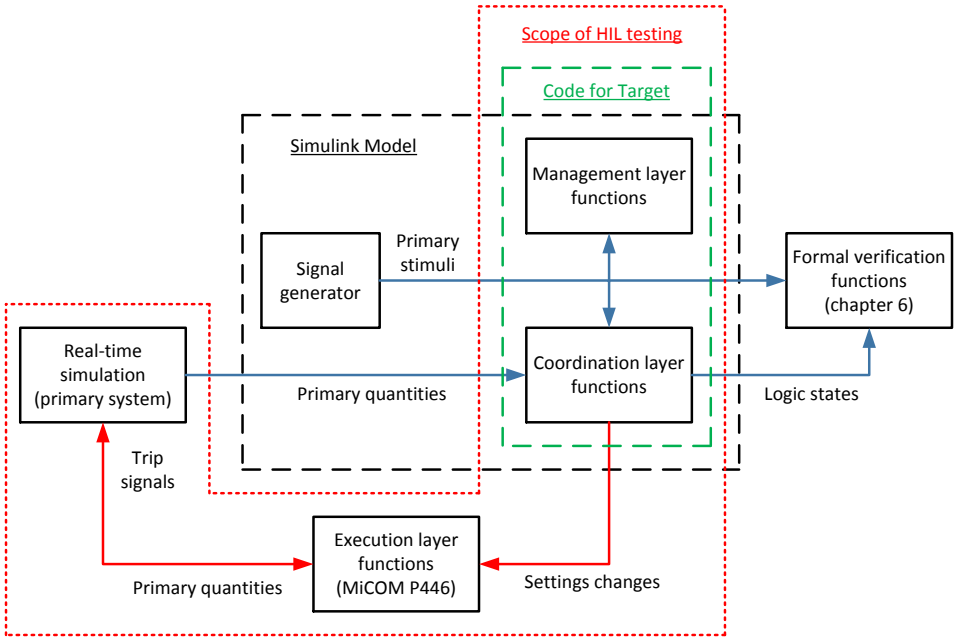

Figure 5-6 High level structure of the Simulink model and interaction with testing

For validation of the overall scheme, Simulink coder is used to generate C code (from functions defined by the dashed green area in Figure 5-6) for deployment onto the target where it forms part of a hardware in the loop (HIL) test (the scope of this is defined by dotted red area in Figure 5-6). Details of this test are in section 5.6. Formal testing (as will be described in chapter 6) will be conducted on the adaptive functions within the Simulink environment itself. For reference the implementation of the scheme is depicted in Figure 5-7. The target used to implement the adaptive protection functions and communications interfaces is the ABB COM600 substation gateway [18]. Furthermore, the RTDS was used to implement the power system model. The target and RTDS are indicated within the implementation diagram in Figure 5-7. The physical equipment used for implementing the adaptive distance protection scheme and testing environment is shown in Figure 5-8. The following subsections describe the implementation of the coordination and management layer and associated functions and communications interfaces.

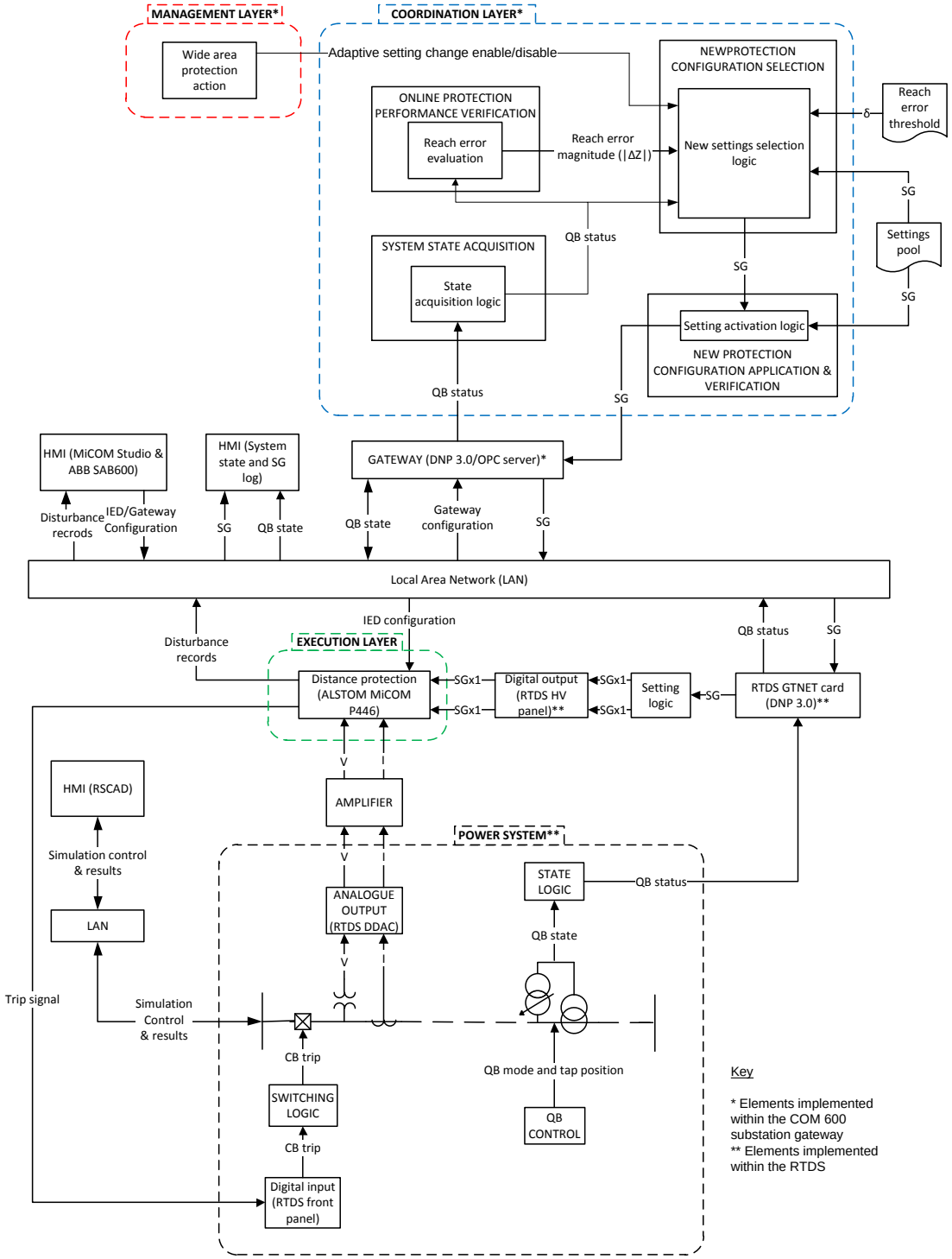

Figure 5-7 Adaptive distance protection scheme implementation

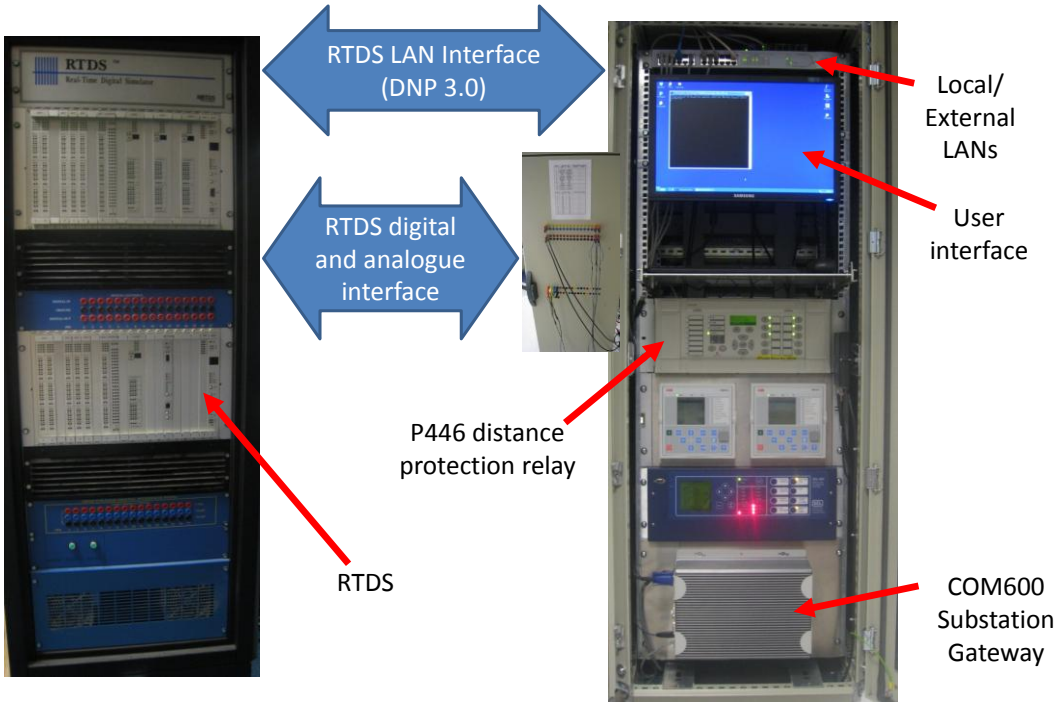

Figure 5-8 Physical equipment used for HIL testing of the adaptive distance protection scheme

5.5.1 Primary 'system state acquisition' function

In this case the adaptive protection functions monitor the primary system quantities that may require an adaption of settings. These quantities are based on indications derived from the following events:

- Change of QB connection (bypassed or engaged): reach errors may be introduced due to this change. The source of this information is the QB controller in the RTDS simulation
- Change of QB mode (boost or buck): reach errors may be introduced due to this change. The source of this information is the QB controller.
- Change of QB tap position: reach errors may be introduced by this change. The source of this information is the QB controller.

Simulink Stateflow has been used to enumerate the QB status based on the measured quantities above. Figure 5-9 shows the Stateflow diagram for acquiring the QB connection and mode status.

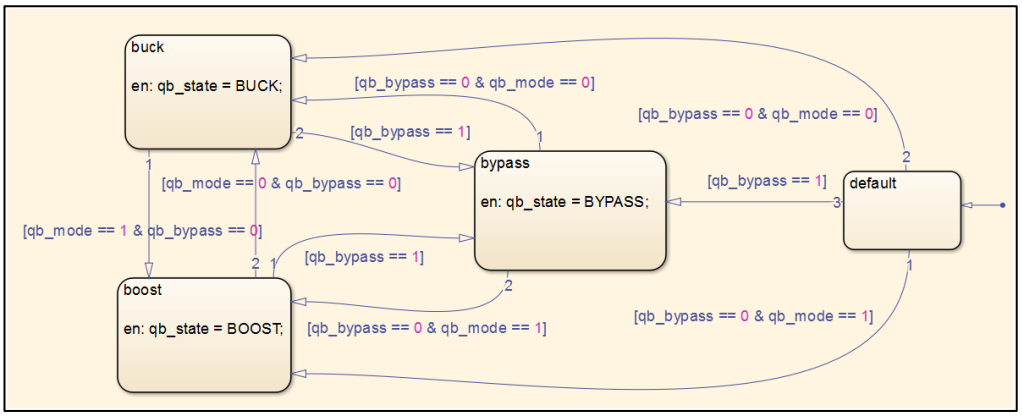

Figure 5-9 QB connection and mode state acquisition

There are two approaches to determining the above changes when the adaptive scheme is operational. The first approach requires regular polling of the sources of information identified above. The second approach relies on the sources of information broadcasting the status change events as soon as they change. The first approach is implemented in this case. When regular polling is utilised, the amount and frequency of data is more deterministic. This is helpful when determining the minimum requirements for the communications networks that carry this data. Furthermore, regular polling is inherently more robust against communications failure as failure to report data during a poll can be an indication of potential communications or component failure. Whereas if event reporting is used, the absence of data reports does not necessarily reflect the health of communications channel or data sources.

5.5.2 'Online protection performance verification' function

The operation of this function is based on the quantification of QB impact on distance reach performance presented in chapter 3. Thus QB state information is used to assess the performance of the distance protection at any given time. In other words, it determines whether reach errors occur as a result of primary system changes, whether these errors are acceptable and whether settings changes are required. To ensure flexibility in the implementation, this function relies on two configurable error 'settings'. This means that the function can be applied to scenarios where the impact on distance protection reach requires fine tuning due to different QB parameters or indeed different kinds of FACTS

devices with a similar impact (e.g. phase shifting transformers, line compensation, etc.). These settings are the reach error magnitude |ΔZ| and the reach error threshold δ. The value of |ΔZ| is determined by the relation presented in chapter 3 (section 3.4.5) which is empirically derived from the offline evaluation of the circuit in question. While δ determines the 'buffer zone' before an error becomes significant and thus triggers a change in settings. An error is deemed significant if the measured impedance lies out with the appropriate protection zone which does not occur for all reach error values. This depends on the network in question. These configurable error settings mean that the adaptive protection response can be characterised given that the inputs and the reach error relations are known. This is beneficial when testing the scheme since the adaptive protection response can be verified against an expected response that is based on this characterisation.

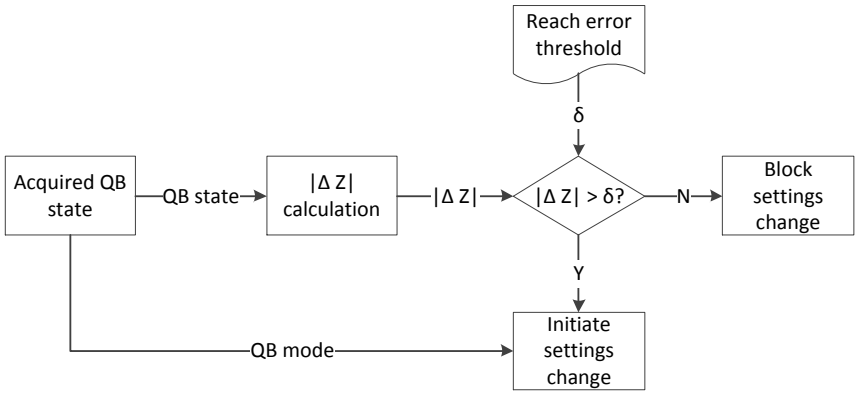

Figure 5-10 Initiating or blocking settings changes based on reach error for a given QB state

5.5.3 'New protection configuration selection' function

Three settings groups were implemented as discussed in the previous chapter and presented here again in Table 5-1 for convenience. This presents the pool of settings that the settings selection logic draws from once triggered to do so.

Table 5-1 Implemented settings groups

SG	Protection zone	Reach (Ω)	Time delay (S)
1 (default)	Zone 1	0.994	0
	Zone 2	3.918	0.5
	Zone 3	7.663	1
2	Not used		-
3	Zone 1	0.994	0
	Zone 2	4.3	0.5
	Zone 3	7.663	1
4	Zone 1	0.994	0
	Zone 2	5.5	0.5
	Zone 3	11.4	1

5.5.4 'New protection configuration activation and verification' function

The newly selected settings groups are written to the communications channel for activation using the communications gateway interface described in the following subsection. The low level implementation of the settings group activation logic is depicted in Figure 5-11. This translates the enumerated settings groups into signals for activation on the distance relay.

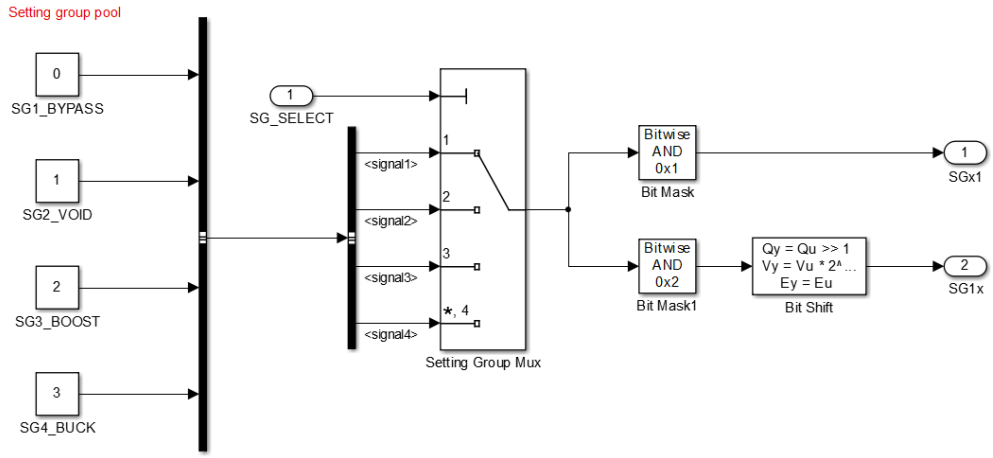

Figure 5-11 Settings activation low level implementation

5.5.5 Implemented communications interfaces

A substation gateway (ABB COM600) has been used to provide the communications capability for transferring data between the RTDS and the adaptive protection scheme [18]. DNP 3.0 was used to exchange this data via the RTDS GTNET card [19]. The gateway utilised an OPC (object linking and

embedding for process control) server to achieve the communication. This presented limitations in the speed and frequency of data exchange as will be seen in the testing results later on. When reading and writing data from and to the OPC server (QB status and setting group respectively), synchronous read/write operations were used which guarantee order of operation but are slower compared to asynchronous read/write operations. Furthermore, the frequency of read/write operations had to be reduced to once every 5s, otherwise software exceptions would occur. An excerpt of the synchronous write operation to activate a new settings group is shown below.

```
switch (setting_group)
{
  case 1: sg_x1.iVal = 0;
        sg_1x.iVal = 0;
        break;
  case 3: sg_x1.iVal = 0;
        sg_1x.iVal = 1;
        break;
  case 4: sg_x1.iVal = 1;
        sg_1x.iVal = 1;
}
writableItem2->writeSync(sg_x1);
writableItem3->writeSync(sg_1x);
```

5.5.6 Management layer functions implementation

A discussed in chapters 3 and 4, national coordinated QB control functionality forms the link between the system operator and the adaptive protection functions. In this case, this link is realised through the management layer. Implementing a coordinated system wide QB control scheme is out with the scope of the thesis. In this case, only the global configuration constraint (see Figure 5-5) has been implemented as an enable signal for coordination layer functions.

5.6 Hardware in the loop (HIL) adaptive distance protection scheme validation

5.6.1 HIL validation methodology

Dynamic testing of the developed adaptive distance protection scheme has been conducted using hardware in the loop arrangement. This has already been illustrated in Figure 5-7. The scenarios that have been tested are summarised in Table 5-2. The tests presented are for phase to phase faults which cause the worst case under reach. Three sets of results are presented for each of the test cases:

- A control case: this shows the response of the distance protection IED without adaptive functionality. The QB status is shown for each case.
- Adaptive protection response: this shows the response of the distance protection IED with adaptive protection functions enabled. The QB status and settings groups selected for each test are also shown.
- IED disturbance record: the record shows the relay trip commands of the individual distance protection zones.

Table 5-2 Summary of hardware in the loop test cases for the adaptive protection scheme

Test case	QB mode	Tap position	Fault position	Tested zone	Fault type
1	Boost	4	50%	Zone 2	Two phase fault
2	Buck	4	30%	Zone 2	
3	Buck	5	50%	Zone 2	
4	Buck	1	70%	Zone 3	
5	Buck	4	100%	Zone 3	

The primary system used for testing is the same one illustrated in Figure 3-6 which was used originally to determine the impact of QBs on distance protection reach. Figure 5-12 shows a section of this network with the simulated fault positions indicated. For scenarios testing zone 2, the simulated fault duration was 0.8s. This duration is increased to 1.3s for zone 3 test scenarios.

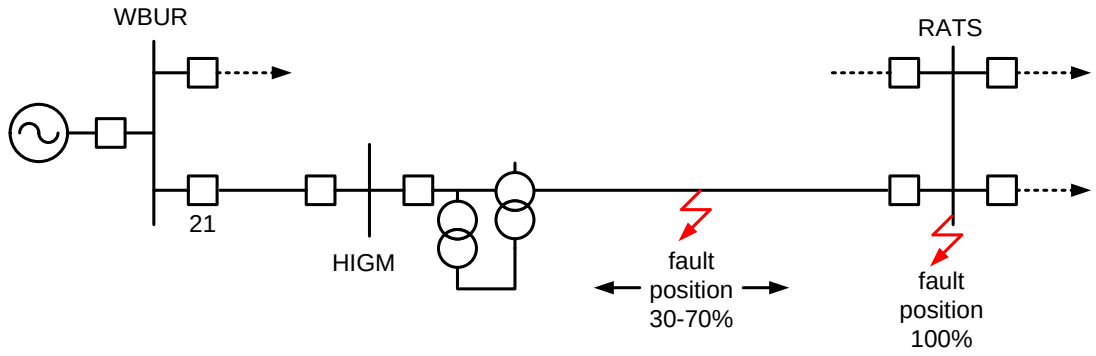

Figure 5-12 Test network showing fault positions and distance protection relay

With adaptive protection disabled, the total simulation time captured is 2s. This is increase to 40s for when the adaptive protection is enabled. This is to ensure that enough time is made available for the OPC server to propagate the QB status and settings changes as discussed previously. Also the plot sampling in RSCAD was reduced to every 8th sample to remain within the maximum limit of available samples for plotting waveforms over a longer period of time. Therefore the resolution of the captured waveforms is slightly reduced as a consequence of increased simulation time – this does not affect the fidelity of the secondary injection.

5.6.2 HIL validation results

5.6.2.1 Test case1 results

Figure 5-13 shows the failure of the distance relay to detect the fault by the absence of the trip signal. Under normal circumstances zone 2 is expected to trip after a time delay of 0.5s.

In Figure 5-14, the adaptive functions are enabled. After engaging the QB at 10s, the active settings group is changed to SG3 at 24s. A fault is applied at 35s which is cleared after the 0.5s zone 2 delay. The associated disturbance record shown in Figure 5-15 confirms the tripping of zone 2 while the other zones do not trip.

When the QB is engaged at 10s, a transient inrush current can be observed (Figure 5-14). This can be avoided by switching in the QB at minimum tap and then gradually tapping up the transformer to achieve the desired tapping position. However, this would have increased simulation time further.

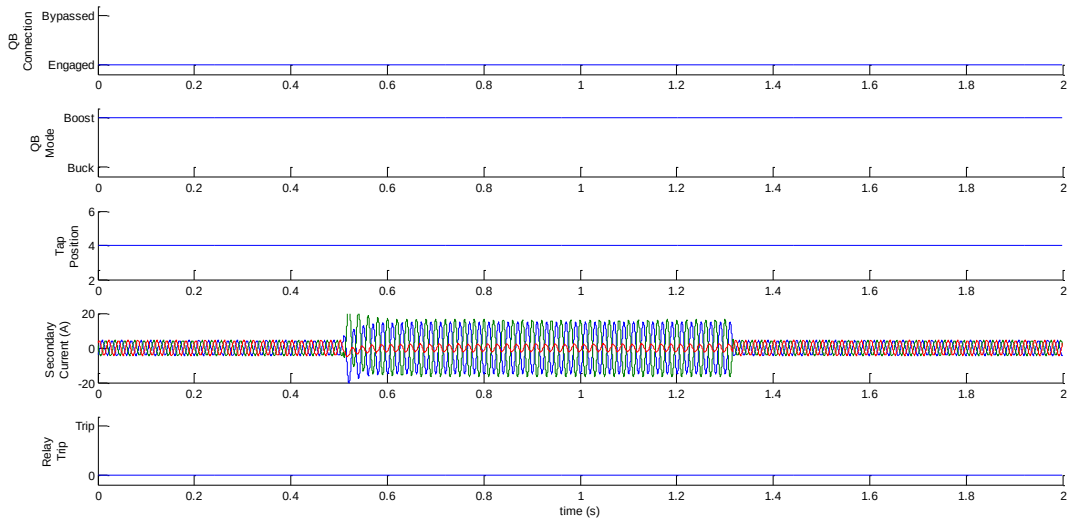

Figure 5-13 Test case 1, adaptive protection disabled

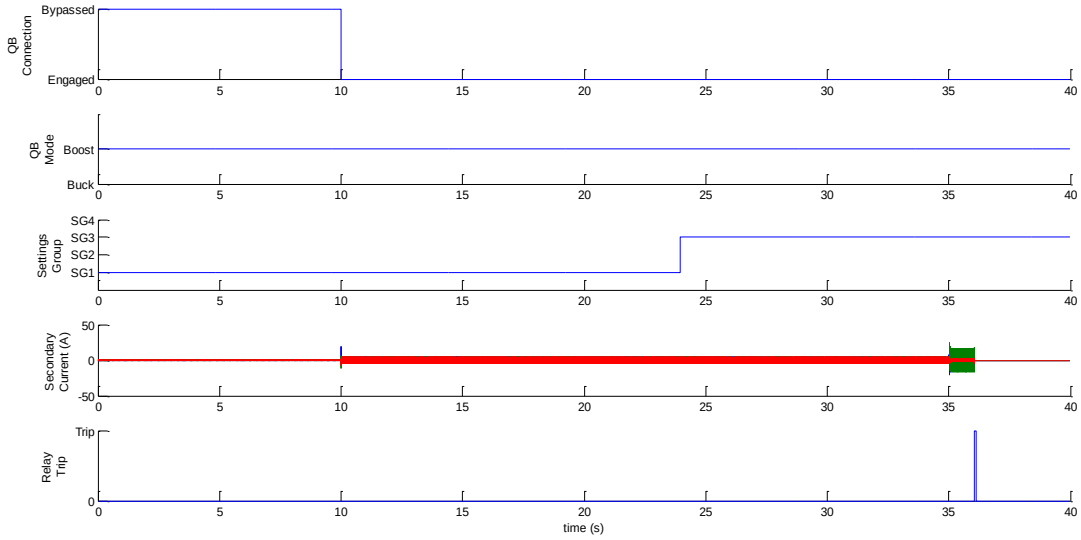

Figure 5-14 Test case 1, adaptive protection enabled

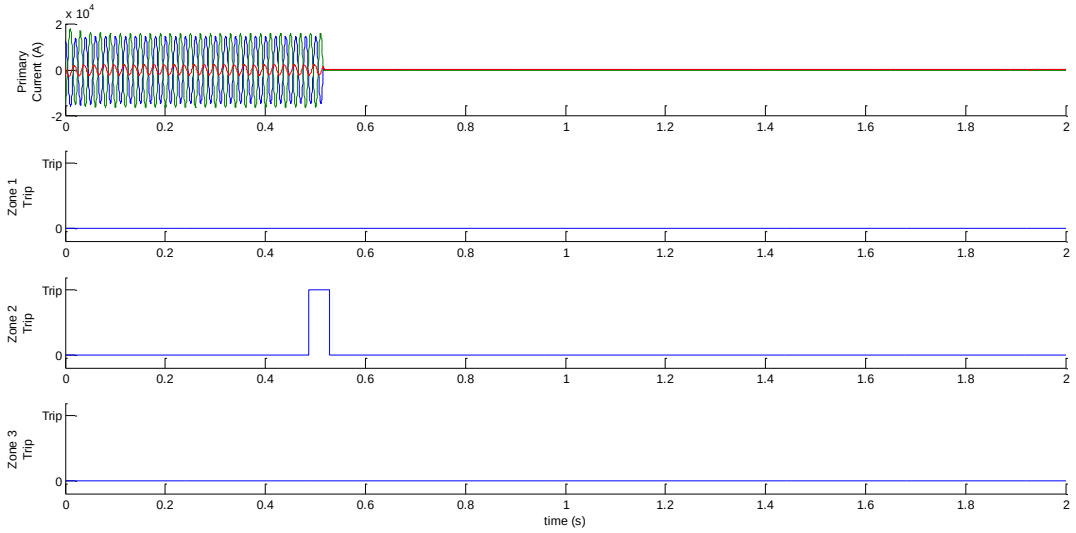

Figure 5-15 Test case 1, IED disturbance record

5.6.2.2 Test case 2 results

In a similar fashion to the previous case, Figure 5-16 shows the failure of the distance protection to trip for an in-zone 2 fault when adaptive functionality is disabled. A correct operation of the relay is obtained when the adaptive scheme is enabled as shown in Figure 5-17. In this case, the settings change takes 19s to take effect. The associated disturbance record where zone 2 trips is shown in Figure 5-18.

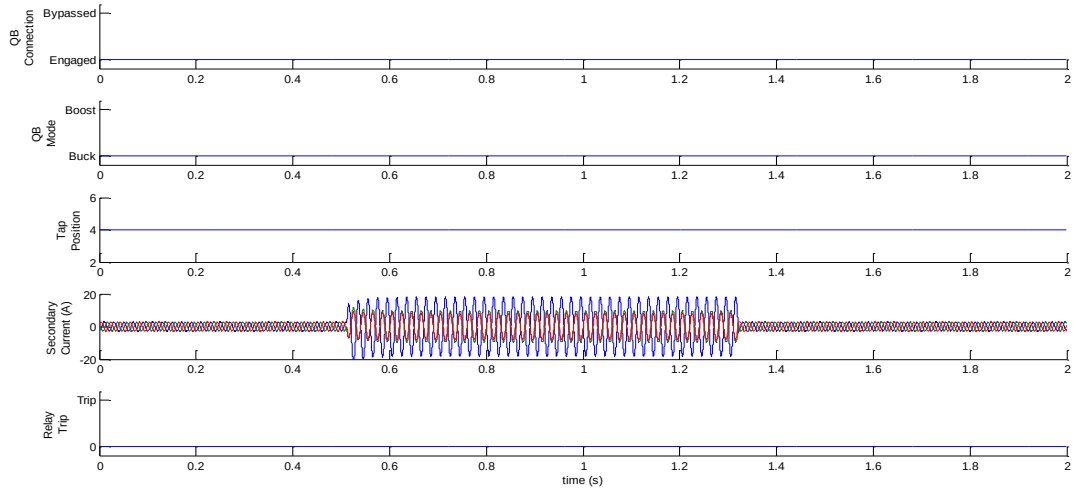

Figure 5-16 Test case 2, adaptive protection disabled

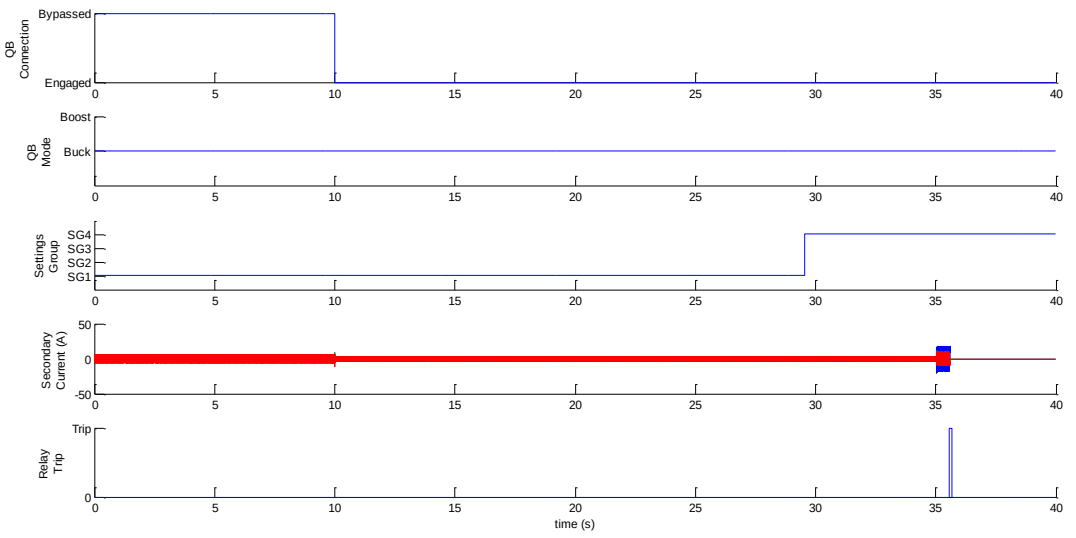

Figure 5-17 Test case 2, adaptive protection enabled

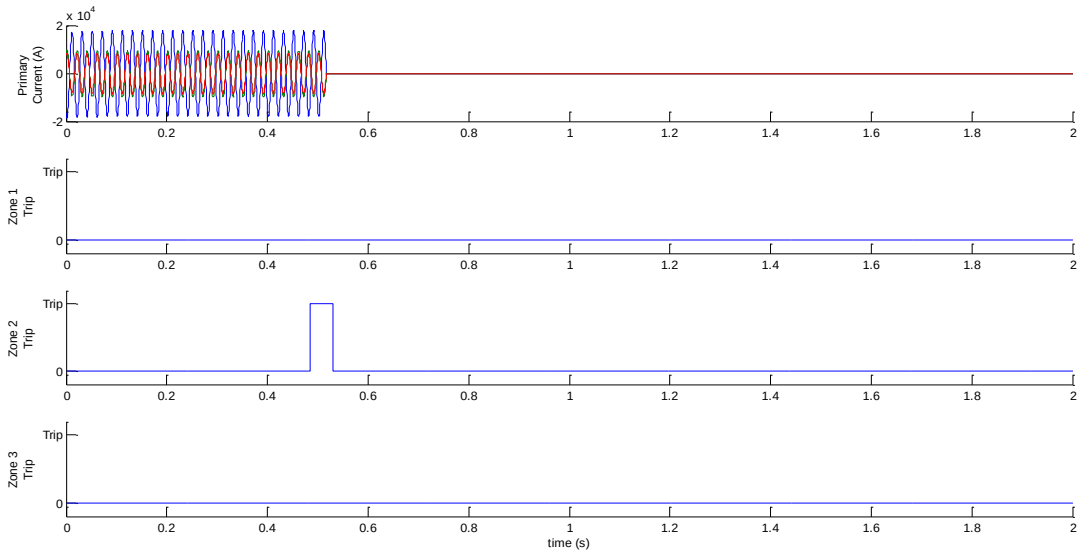

Figure 5-18 Test case 2, IED disturbance record

5.6.2.3 Test case 3 results

The final test case for zone 2 operation is shown in Figure 5-19 when adaptive protection is disabled. Correct operation of the zone 2 relay is obtained and depicted in Figure 5-20 where the settings change takes effect in 14s. The associated disturbance record is shown in Figure 5-21.

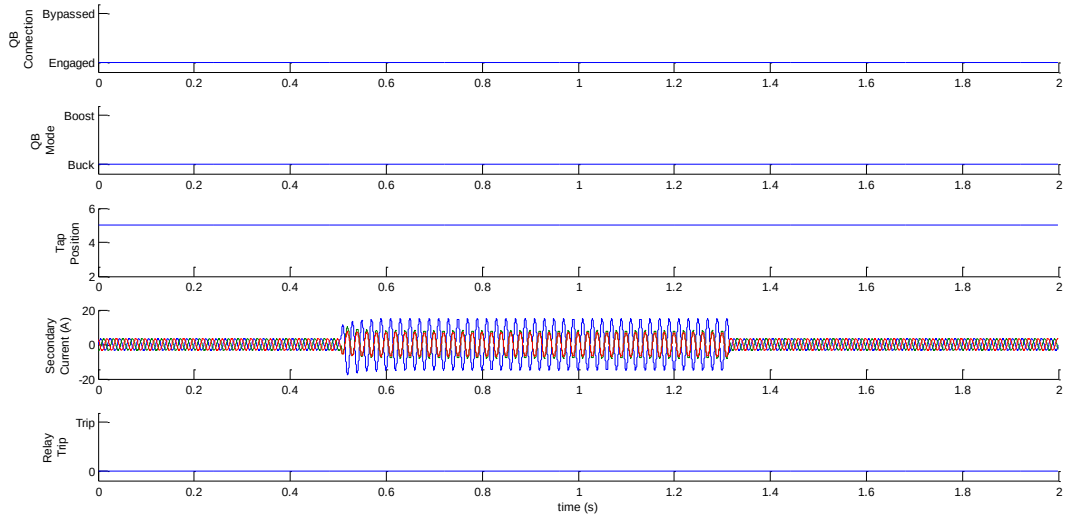

Figure 5-19 Test case 3, adaptive protection disabled

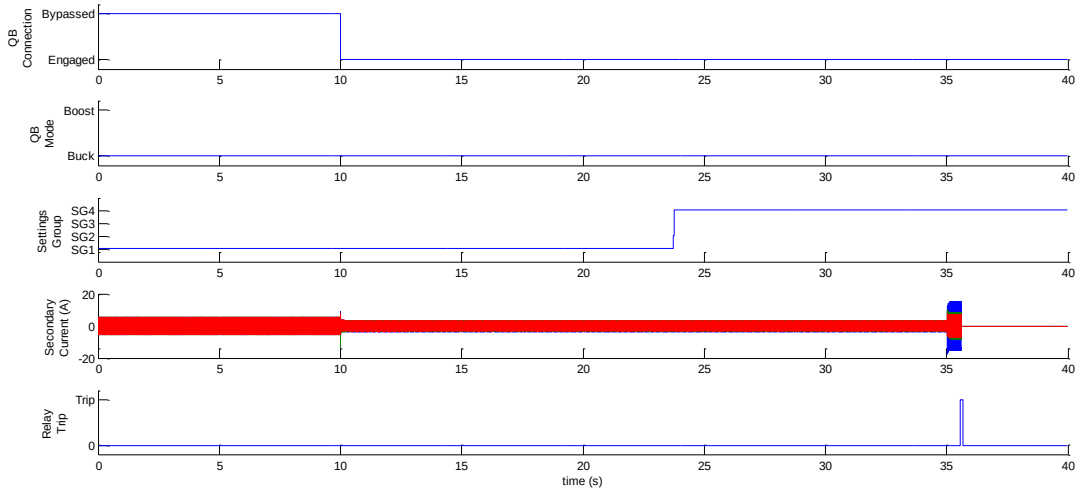

Figure 5-20 Test case 3, adaptive protection enabled

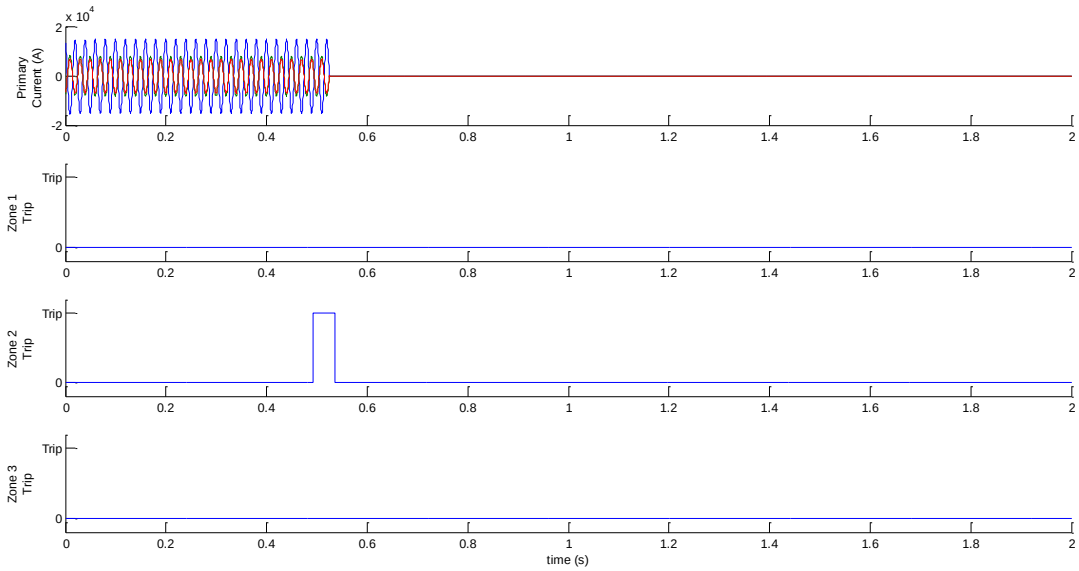

Figure 5-21 Test case 3, IED disturbance record

5.6.2.4 Test case 4 results

Zone 3 operation is tested in this case. Figure 5-22 shows that the relay fails to trip for an in zone fault when adaptive functionality is disabled. Successful fault clearance post adaptive settings group change is shown in Figure 5-23. In this case, the settings changes took 16s to take effect. The relay trips after 1s zone 3 time delay. The associated disturbance record is shown in Figure 5-24.

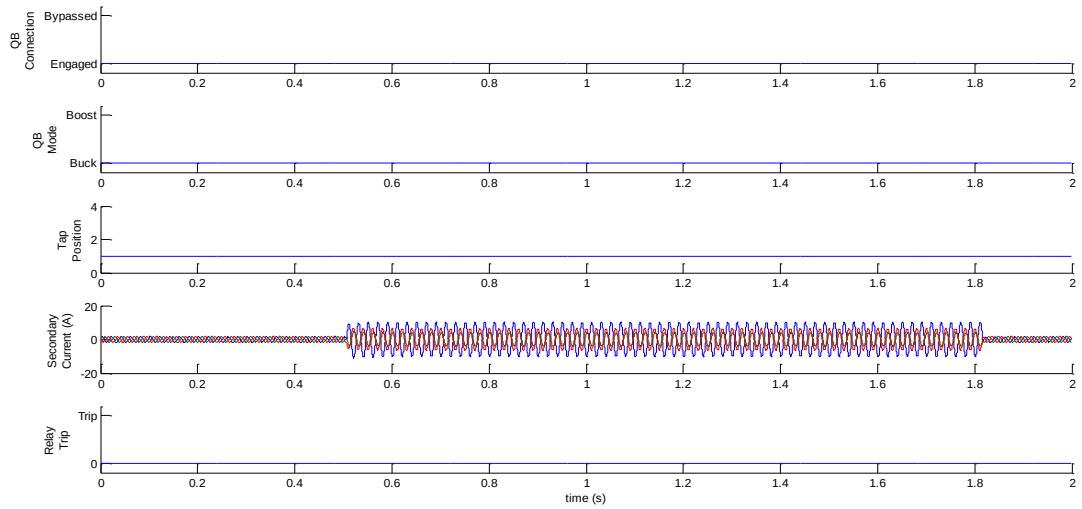

Figure 5-22 Test case 4, adaptive protection disabled

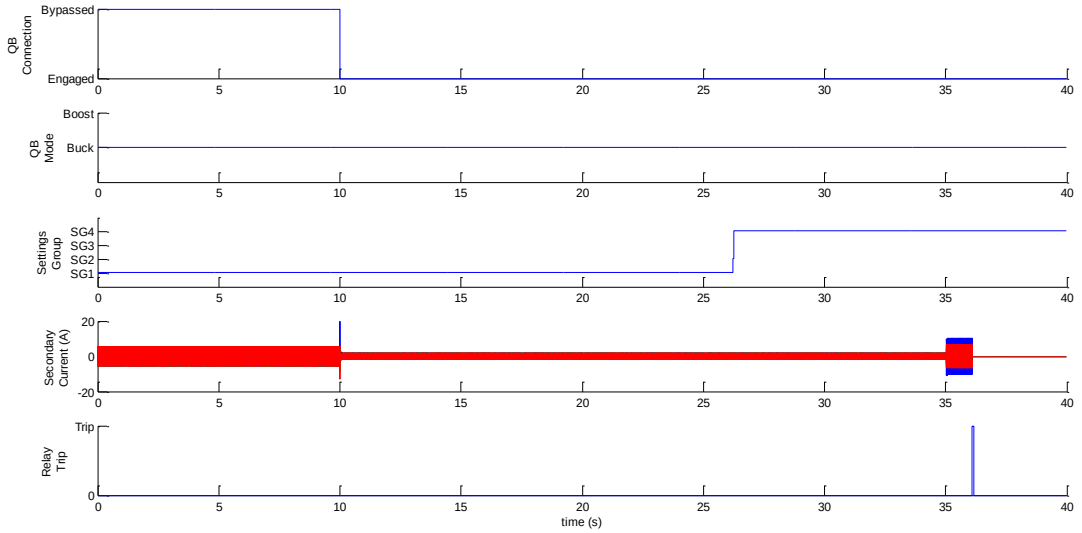

Figure 5-23 Test case 4, adaptive protection enabled

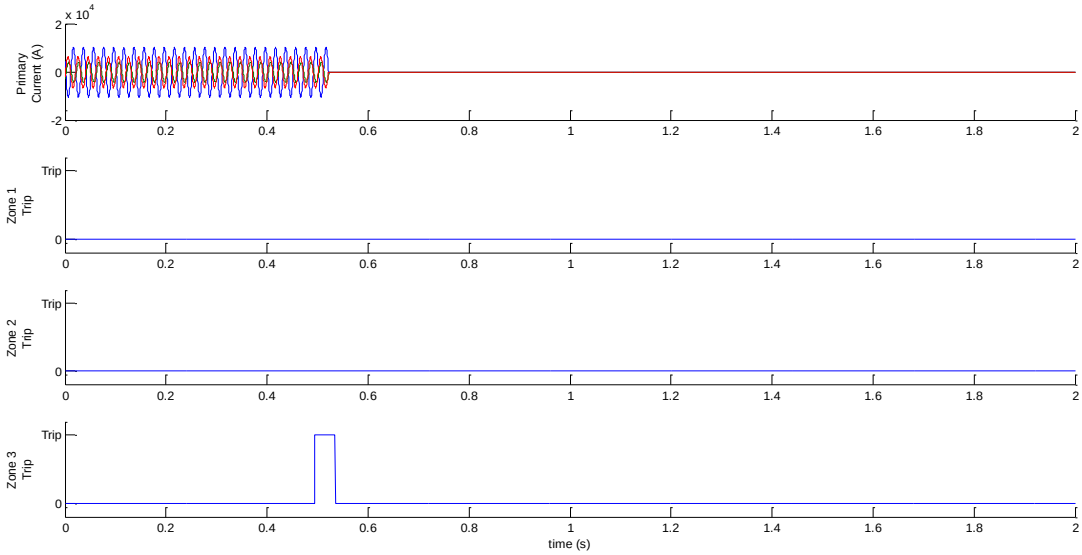

Figure 5-24 Test case 4, IED disturbance record

5.6.2.5 Test case 5 results

The final zone 3 test case is shown in Figure 5-25 - Figure 5-27. Successful zone 3 operation is obtained with setting change taking 15s to be activated.

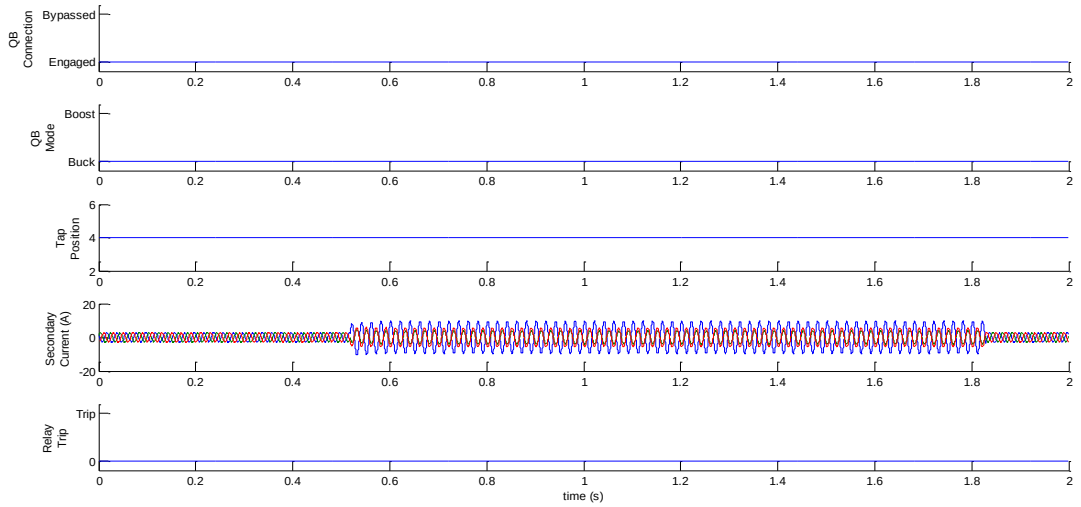

Figure 5-25 Test case 5, adaptive protection disabled

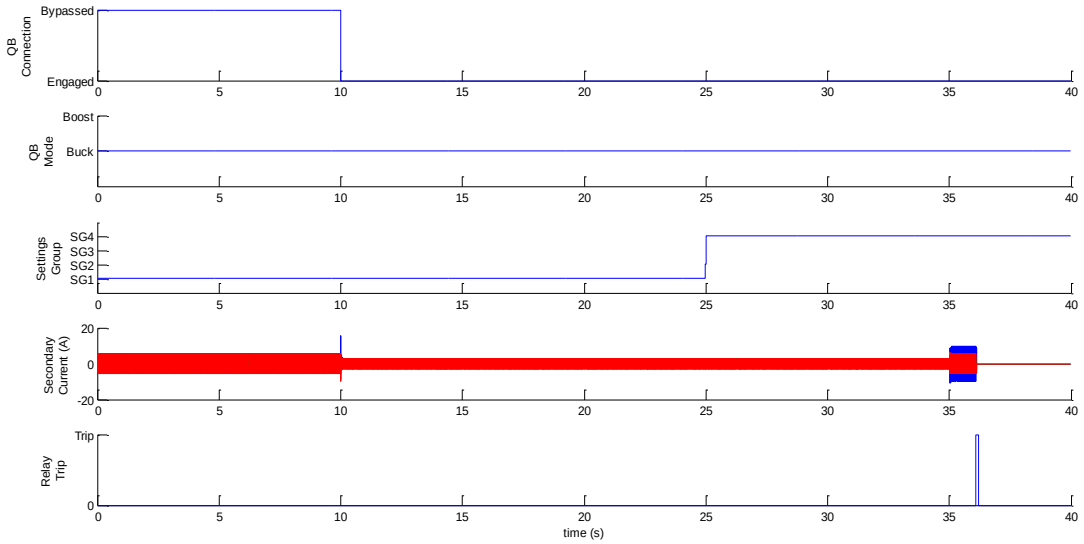

Figure 5-26 Test case 5, adaptive protection enabled

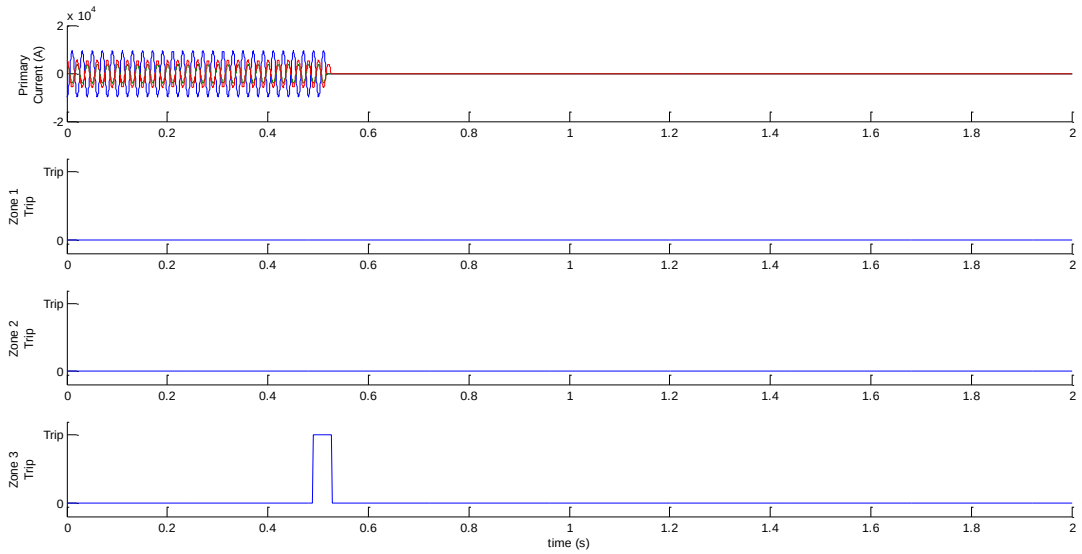

Figure 5-27 Test case 5, IED disturbance record

5.6.3 Discussion of HIL validation results in light of APA design and scheme implementation

In view of the validation results obtained in the previous section, the following three main issues will be examined:

- The time delay associated with the settings group changes.
- The performance impact of adaptive protection functions interactions on that of the conventional protection functions.
- Implementation constraints of prototype vs. production adaptive protection schemes.

The results have shown that a changing between settings based on the implementation of the scheme takes 14-19s from the point at which the primary system changes. As discussed earlier, this variability is due to the use of the synchronous read/write operations for the OPC server. Although asynchronous operation can provide better performance, the synchronous approach offers a critical feature. This feature is the guarantee of order read/write operations. The order in which read (system state acquisition) and write (settings activation) operation are performed is important from the point of view of reliable and deterministic adaptive protection functionality. The APA specifies that these operations are performed in a certain order to fulfil the required functionality. As such, an incorrect setting may be selected temporarily until the

status values settle. Therefore, the synchronous approach offers a form of 'logical interlocking' when attempting to change settings groups.

Not acting to primary system changes with the appropriate settings leaves the back-up protection vulnerable to reach errors. The duration of this vulnerability has been reduced by applying the adaptive protection functions. In this particular case, a delay of 14-19s in new settings activation should be acceptable as it is unlikely that the QB would change states at a rate faster than this delay. Generally speaking, however, there leaving the primary system in a degraded protection state may not be acceptable especially when the system is operating in a stressed state. This is where management layer functionality becomes more important. The ability to determine the stressed state of the system, coupled with predictive state estimation capabilities, enables adapting relays most at risk. Once target relays are identified, new settings can be pre-determined but only activated once the need for a change occurs from the power system point of view. Thus reducing the time required for changes to take effect.

The use of industry standard communications gateways (ABB COM600) to host the adaptive protection functions and required data communications facilitates their integration into digital substations. However, the APA dictates that the deployment of these functions is platform agnostic. This should be taken into account when planning the migrating of the developed adaptive functionality from a prototype phase to a production (substation-ready) phase. As such, experience with the prototyping phase must dictate the requirements for the next generation of relaying platforms including faster (and more reliable) data exchanges at the interface between the coordination and execution layers.

The APA dictated that the performance of existing protection relays (as set) is preserved by specifying the functional separation between execution and coordination layers. This has been validated in the results. The action of the adaptive functions did not interfere with the operating time of the distance protection zones. Indeed, the reach of the relays has been improved by the

adaptive functions when the QB was in use. The APA further ensures that the execution layer performance (as set) is unaffected by inherently limiting the frequency of interactions between it and the coordination layer. This is achieved by dictating that the nature of information the coordination layer reacts to is of a discrete nature Consequently, marginal changes in the power system do not cause continuous new setting activation requests or potential 'hunting' in the process of doing so.

5.7 The role of hardware in the loop approach to validating adaptive protection schemes

The previous section demonstrated how HIL testing can be used to validate the performance of the overall scheme while incorporating all the elements of the adaptive protection functionality as well as the primary system components. One of the major advantages of this approach is the ability to unearth issues with system integration especially those stemming from the exchange of information between the constituent elements of the scheme and the power system. However, one of the inherent issues with HIL is that there is a major dependency on the design of test cases. In other words, observations obtained from the testing are limited by the scope of test scenarios and their ability to sufficiently stimulate a wide spectrum of responses from the adaptive protection functions. With an adaptive protection scheme in place, measures must be taken to ensure that levels of confidence in their performance derived from testing are similar to those for conventional schemes. This level of performance should be consistent for all network operating conditions that the adaptive scheme reacts to. Furthermore, HIL testing remains a black box approach to the testing which may not reveal performance issues at the algorithm level. Examining the behaviour an adaptive protection algorithm more closely is important as it is generally less understood compared to well established conventional protection algorithms.

To this end, a complementary methodology to the testing of adaptive protection schemes will be examined in the following chapter. This is based on a more formal approach to the testing which utilises the characterisation of the

behaviour of the adaptive functions under different network operating conditions. It is important to emphasise the different approaches to the testing, as will be seen, should be complementary to capitalise on the strengths of the different approaches to the testing. One of the main questions that remain, however, is how much emphasis should be placed on each approach?

5.8 Chapter summary

This chapter presented the engineering process of the design, implementation and testing of adaptive protection schemes. This is a requirements driven process which takes into account the different lifecycle stages an adaptive protection scheme goes through. To facilitate the design and implementation, a previously proposed architecture (structural model) for adaptive protection scheme has been further developed to formally define the required interactions to achieve acceptable scheme performance. The architecture elements were then realised through the model-based design and implementation of a prototype adaptive distance protection scheme. A hardware in the loop (HIL) approach was used to validate the overall scheme performance in terms of reach selectivity under different QB operating scenarios. The scheme proved successful in compensating for the under reach caused by QB operation. By design (settings group range), zone 2 reach compensation is limited to up to 20% in order to avoid mis-coordination with adjacent lines. The implementation and testing focussed on the coordination and execution layer functions. To this, end the relevant parts of the architecture have been validated for a transmission level protection application. This can be generalised to applications involving FACTS devices with an impact on distance protection that can be characterised with high certainty. Furthermore, the HIL approach to testing can be limited by the design of the test case. Therefore it was recommended that further testing of a different nature is required to reveal any performance shortfalls in the scheme not immediately observable via HIL testing and this will be discussed in the following chapter.

5.9 References

[1] R. Tumilty, "A Study of Adaptive Protection Methods for Future Electricity Distribution Systems," PhD Thesis, 2013.

[2] R. Stevens, *Systems engineering: coping with complexity*: Pearson Education, 1998.

[3] Adrianti, I. Abdulhadi, A. Dysko, and G. Burt, "Assessing the Reliability of Adaptive Power System Protection Schemes," in *Developments in Power System Protection (DPSP 2012). Protecting the Smart Grid, 11th IET International Conference on*, 2012.

[4] IEC, "IEC 61850: Communication networks and systems in substations," ed, 2003.

[5] C. M. De Dominicis, P. Ferrari, A. Flammini, S. Rinaldi, and M. Quarantelli, "On the Use of IEEE 1588 in Existing IEC 61850-Based SASs: Current Behavior and Future Challenges," *Instrumentation and Measurement, IEEE Transactions on,* vol. 60, pp. 3070-3081, 2011.

[6] IEEE, "IEEE Standard for System and Software Verification and Validation," *IEEE Std 1012-2012 (Revision of IEEE Std 1012-2004),* pp. 1-223, 2012.

[7] B. Kirby, L. Zou, J. Cao, I. Kamwa, A. Heniche, and M. Dobrescu, "Development of a predictive out of step relay using model based design," in *Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on*, 2011, pp. 1-6.

[8] IEC, "IEC 60255: Measuring relays and protection equipment," ed, 2010.

[9] I. Abdulhadi, F. Coffele, A. Dysko, C. Booth, and G. Burt, "Adaptive protection architecture for the smart grid," in *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies (ISGT Europe)*, 2011, pp. 1-8.

[10] M. Khederzadeh and T. S. Sidhu, "Impact of TCSC on the protection of transmission lines," *Power Delivery, IEEE Transactions on,* vol. 21, pp. 80-87, 2006 2006.

[11] Z. Q. Bo, F. Jiang, Z. Chen, X. Z. Dong, G. Weller, and M. A. Redfern, "Transient based protection for power transmission systems," in *Power Engineering Society Winter Meeting, 2000. IEEE*, 2000, pp. 1832-1837 vol.3.

[12] M. Jin and T. S. Sidhu, "Adaptive load encroachment prevention scheme for distance protection," *Electric Power Systems Research,* vol. 78, pp. 1693-1700, 2008.

[13] Y. Xingbin and C. Singh, "A practical approach for integrated power system vulnerability analysis with protection failures," *Power Systems, IEEE Transactions on,* vol. 19, pp. 1811-1820, 2004.

[14] P. Sung-Jun, L. Seung-Jae, C. Myeon-Song, K. Tae-Wan, K. Sang-Tae, and K. Jin-Hwan, "A new index for evaluating protection vulnerability," in *Power and Energy Society General Meeting, 2011 IEEE*, 2011, pp. 1-5.

[15] V. N. Madani, D. Begovic, M. Adamiak, M., "Application Considerations in System Integrity Protection Schemes (SIPS)," ed: GE Digital Energy, 2009.

[16] E. E. Bernabeu, J. S. Thorp, and V. Centeno, "Methodology for a Security/Dependability Adaptive Protection Scheme Based on Data Mining," *IEEE Transactions on Power Delivery,* vol. PP, pp. 1-1.

[17] B. Kirby and H. Kang, "Model Based Design for Power Systems Protection Relays, Using Matlab & Simulink," in *Developments in Power System Protection, 2008. DPSP 2008. IET 9th International Conference on*, 2008, pp. 654-657.

[18] ABB, "ABB COM600 Station Automation - Product Guide," 2009.

[19] RTDS, "RTDS Hardware Manual - GTNET Card," 2009.

6 Formal approach to the verification of adaptive protection scheme performance based on hybrid systems modelling

6.1 Chapter methodology and contributions

Adaptive protection can be effectively tested when its behaviour is formally described and verified against a set of predefined performance criteria. This should take into account interactions between the adaptive scheme and the primary system which ultimately triggers adaptation in the protection behaviour when necessary. This is the underlying hypothesis of this chapter, which requires a formal representation of the behaviour of an adaptive scheme. A formal testing methodology that utilises this representation is then possible.

The previous chapter outlined the different methods that can be used to test an adaptive protection scheme's functionality and performance, but focuses on the overall validation of the scheme. This chapter focuses on the verification of the adaptive protection logic. That is the logic which selects a new protection configuration (a new setting in this case) which suits the primary system's prevailing conditions. By formally modelling the behaviour of the adaptive distance protection scheme presented in previous chapters, the verification of its performance has been shown to be possible. This chapter demonstrates the use of reachability analysis as a means of verifying the safety property of the adaptive protection logic. This is a formal description of 'undesirable' states that the logic may reside in and the possible operational conditions that lead to residing in these states.

The main contributions of this chapter are:

- Development of a novel methodology where the behaviour of adaptive protection functions interacting with conventional protection functions and the primary system is described in the hybrid systems domain. The use of this behavioural modelling approach for the stated application is the first of its kind.
- The standard hybrid system discrete event abstraction has been redefined to overcome limitations in describing hierarchical control structure. This was necessary to encompass the additional control loop introduced by the adaptive protection functionality.
- A unique methodology of conducting the reachability analysis has been developed. This relies on creating two concurrent state spaces of the hybrid system – operational states and performance states. Consequently, a more direct mapping between the active configuration of protection scheme and its behaviour under test can be achieved. The reachability analysis conducted verifies the safety property for adaptive protection schemes (specifically settings selection functions).
- More efficient safety verification of the adaptive protection logic was achieved by eliminating the need for time consuming continuous state space computations. This is possible by inferring the safety state of the primary system from operational and performance states mentioned above.

6.2 Power system modelling in the hybrid system domain

6.2.1 Hybrid dynamical systems overview

Hybrid dynamical systems (HDS) are those systems which exhibit both discrete and continuous dynamics [1]. In such systems, discontinuities in their state space trajectories result in jumps between a set of discrete continuous dynamics. An HDS is represented using an automaton H which is formally expressed in (1) [2]:

$$H = (Q, X, In, Init, f, Dom, E, G, R) \quad (1)$$

Where, $Q = \{q_0, q_1, \dots, q_n\}, n \in \mathbb{N}$ is the set of discrete states, $X = \mathbb{R}^n$ is the set of continuous states, In is the set of control and disturbance inputs, $Init \subseteq Q \times X$ is the set of initial states, $f(q, x): Q \times X \to \mathbb{R}^n$ is the continuous vector field, $Dom(q): Q \to 2^x$ is the discrete state domain, $E \subseteq Q \times Q$ is the set of edges or transition maps, $G(x): E \to 2^x$ is the set of transition guard conditions, and $R(q, x): Q \times X \to 2^X$ is the continuous vector field reset relation.

Hybrid systems modelling is applied to a number of engineering system problems such as air traffic control, highway traffic modelling, manufacturing processes and more recently power systems [3]. Describing such complex systems in this domain allows for the use of formal performance verification techniques where otherwise determining the behaviour of the system can prove difficult or non-conclusive [4]. The study of power systems in the hybrid domain enables determining the primary system performance under different conditions. Usually, hybrid modelling is applied to study power system stability problems. For instance, the impact of circuit disconnection (a discrete event) on the generator stability (a continuous dynamic system) can be determined as discussed in [5]. It has also been used to evaluate the performance of power system controls to avoid system overload through automatic load disconnection [6]. In this case, circuit breaker action is used to indicate the discrete events and transmission line loading represents the continuous dynamics.

In order to analyse the properties of a hybrid system, its dynamics are abstracted using a discrete event system (DES) representation such as that shown in Figure 6-1. The continuous state variables of the plant are monitored for events (discrete transitions). The process of detecting these events is modelled by the event 'generator'. A response is produced by the controller from a set of control actions. These are interpreted by the 'actuator' for application to the continuous plant.

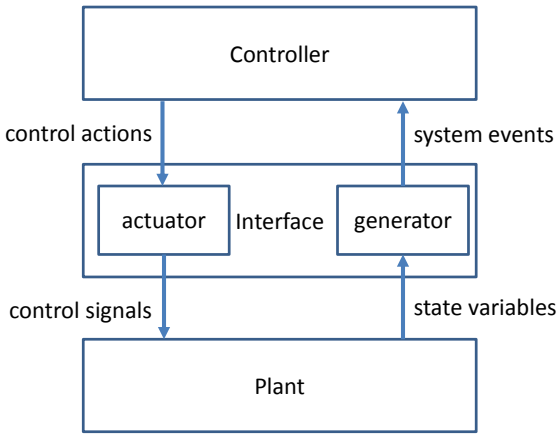

Figure 6-1 Basic DES abstraction of a hybrid system [1]

6.2.2 Modelling power systems in the hybrid domain

To apply the automaton of (1) in a power system context, the general model can be adjusted to deal with the specific system being analysed. In the case of power system stability, for instance, the field vector can represent the angular or voltage stability dynamics and examples of their formulation can be found in [5] and [7] respectively. In these papers, generator swing dynamics were used to capture the power system continuous dynamics and these were varied with different fault and network topology conditions, hence represented by different discrete states. Furthermore, protection action was used to trip certain lines in the power systems to mitigate potential stability issues as identified by the evolution of the continuous state space. [6], [8], [9] and [10] illustrate the transitions between discrete states describing the states of a transmission line as a result of protection operation as well as the transition between power system operational states. In these papers, the hybrid system model was

realised using the Simulink Stateflow toolbox. The model included line loading dynamics and dynamics of an overcurrent relay. A controller that responds to the line loading conditions was developed to perform emergency load shedding if transmission circuits become overloaded post fault conditions. The work in [11] incorporates the action of a transformer tap changer into the primary system model and its effect on the system voltage profile. The hybrid system representation has also been applied to marine electrical systems for the design of network reconfiguration controllers that deal with failures [12]. In this paper, faults in the marine network are monitored and an appropriate action is taken post fault including network topology changes, reduction in propulsion, shedding of loads, etc. The actions depend on the nature of the fault and its impact on the marine network while trying to maintain as much power as possible to critical loads. Modelling the power system in the hybrid systems domain is an emerging area of research interest with promising applications to the verification of the said systems' performance under dynamic conditions. Furthermore, formulating the behaviour of the system through a hybrid model enables a bottom up approach for synthesising stable and robust controls [13].

It is clear from the literature that the nature of the hybrid model allows for encompassing primary and secondary system dynamics simultaneously. However, the extent to which the size and complexity of the power system model that can be elaborated remains unclear. This is mainly due to the limited sizes of networks being presented and the limited actions of the controllers being designed. The scope of the network used in this chapter's case study does not exceed those presented in the literature. Furthermore, the actions performed by the adaptive protection logic (developed in the previous chapter) are well defined in a handful of settings groups options, and do not have a direct impact on the evolution of the dynamic state variables of the primary system. Thus there is no evidence that the methods proposed for power system applications in the literature will place limitations in terms of state formulation for the adaptive system case study. However, there are limitations in terms of interaction formulations that need to be overcome and will be examined further

in a later section. Although the literature examined the interactions between protection and power system, to some extent, in the hybrid systems domain, no attempt has been made to incorporate the actions of adaptive protection – this is the focus of this chapter.

6.3 Verification of hybrid systems performance

The ability to determine the performance of complex dynamic systems through hybrid modelling has proven to be an advantage. The performance of a hybrid system can be verified by applying certain analysis techniques [14]. Such performance measures include (with possible power system applications):

- **(Transition) stability**: discrete state transitions should not be affected by small perturbations in the continuous system state. Incorrect protection operation can be an example of instability in determining the system state.
- **Controllability**: the ability to obtain any target state from any initial state within a finite time using control action. This applies, for example, to the use of FACTS devices for dampening system oscillations to direct the power system to a more stable state.
- **Determinism**: the ability to determine the next state given the current state and input. Ideally, when a short circuit occurs then the protection can reliably detect the fault and isolate it given that the fault conditions satisfy the protection characteristics and logic.
- **Observability**: the ability to determine the system state by observing its outputs over a period of time. This can apply to power system state estimation, or more recently, wide area measurement systems that can determine the power system state by performing key measurements.
- **Safety/reachability**: the ability to determine whether an unsafe state is reachable from an initial state. For instance, would the onset of a system fault lead to instabilities or eventually a blackout?

6.3.1 The use of reachability analysis to verify hybrid system safety

In order to conduct reachability analysis, it is first necessary to partition the hybrid system's state space in safe and unsafe regions. This is then followed by monitoring the state transitions and continuous state trajectory to determine whether these unsafe regions are reached or that the system resides in the safe regions at all times.

It is generally necessary to explicitly compute the complete state space in order to determine the unsafe regions within it [15]. In order to determine whether these regions are reachable, then either forward or backward reachability can be applied [4]. In forward reachability, initial conditions (states) are set then inputs are applied to the system to determine whether the unsafe sets are reached. Alternatively, in backward reachability, the starting set is the unsafe state and the system trajectory is observed to check if normal operating states are reached from the initial conditions. Initialising the system can have a role in avoiding or reaching the unsafe state. This is in addition to the role of effective (safe) control action that aims to drive the system away from unsafe states.

Reachability analysis has been applied in power systems applications and has encompassed the action of protection systems. For instance, [3] verifies the safety of fault release control – a form of operational tripping scheme. Should generator disconnection occur, certain transmission lines are tripped in order to avoid angular instability of other generators in the network. Generator angles limits are used as criteria to determine the safe operating region of the power system within the state space. Violating these limits results in loss of synchronism.

In [7], reachability analysis is used to determine whether voltage instability occurs as a consequence of transmission circuit disconnection. This takes into account the automatic voltage control of the generator along with the discrete transitions caused by the disconnection of the lines. The critical value of the bus voltages determines the safety region boundary. Voltage stability is also examined in [16]. Reachability is also used to determine the onset of voltage

instability. However, the paper proposes supervisory control to mitigate its effects by issuing a combination of voltage control measures as appropriate.

6.3.2 Justification for conducting reachability analysis for adaptive protection safety verification

As mentioned earlier, the use of hybrid systems modelling for describing the dynamic behaviour of adaptive protection schemes is a unique application. As such, once an appropriate model has been developed, the performance of the scheme can be verified for one or more of the aforementioned criteria. Reachability (safety) analysis was chosen in this case.

The focus of literature on reachability analysis for power system applications has influenced this decision to some extent. But more importantly, determining the safety of the adaptive protection logic is the most direct measure of potential mal operation due to deficiencies in this logic. As such, reachability is seen as an important first step in establishing a 'toolbox' of formal performance verification methods for adaptive protection.

Furthermore, one of the main difficulties in conducting the reachability analysis is in the requirement to explicitly computing the system's state space. Although an accurate representation of the system interactions is obtained, it may not be necessary for all applications. The remainder of the chapter shows how computing the complete state space is not always necessary if an appropriate abstraction of the behaviour is developed. Once the behaviour of the scheme is modelled, potential safety violations can be inferred from a set of predefined state transitions.

6.4 Defining a hybrid model for the developed adaptive distance protection scheme

In this section, the behaviour of the adaptive distance protection scheme developed in the previous chapters will be formally described using hybrid systems modelling. Interactions between the primary system and the protection scheme will be formulated. The behavioural model from the point of view of the adaptive protection scheme will reflect the response of the settings selection logic to primary and secondary system inputs to the adaptive logic. The process involves developing a suitable DES abstraction and then conducting reachability analysis on the system after defining its safety states based on protection performance criteria.

6.4.1 Developing a DES abstraction to include adaptive protection functionality

6.4.1.1 Components of system under study

Consider the high level structure and interactions of the system under study which comprises the adaptive protection logic, conventional distance protection IED and the protected primary system shown in Figure 6-2. This reflects the adaptive distance protection developed in the previous chapter.

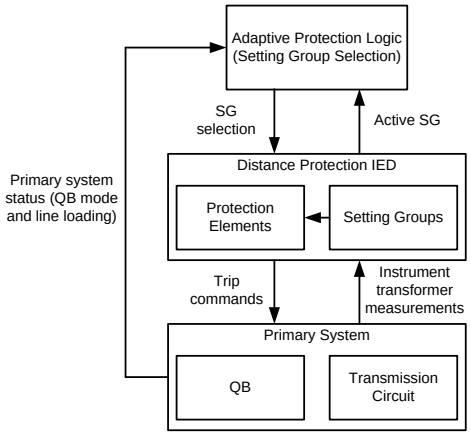

Figure 6-2 System under consideration for behavioural modelling

A DES abstraction represents a continuous piece of plant and a discrete controller. In this case, the continuous plant largely represents the power system dynamic behaviour such as line loading. Discrete dynamics in this case

represent the QB transformer status including the tap position. The operation of circuit breakers has no bearing on the adaptive protection logic. Problems in formulating the overall system behaviour arise when attempting to integrate the adaptive protection functionality into the model. These functions act on the protection relay which is considered a discrete controller in its own right. Furthermore, the adaptive protection functions rely on measurements from both the power system and the conventional protection elements. None of the DES implementations found in the literature represent control structures of this hierarchical nature. The first step in overcoming this issue is to examine the dynamics and the interactions of the subsystems involved – that is the primary system, the conventional secondary system and the adaptive secondary system. It is emphasised that the term secondary system is used in this case not only to preserve the generality of the model, but also to encompass the control IEDs which are used to extract status information related to QB status and circuit breakers.

The conventional secondary system comprises mainly of the conventional protection elements and the primary plant controllers. The protection elements themselves exhibit both discrete and continuous dynamics. To explain this, consider a simplified distance protection element which is depicted in a finite state machine in Figure 6-3.

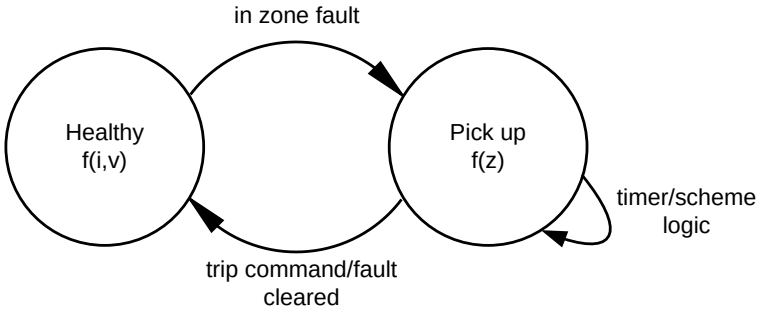

Figure 6-3 Finite state machine representing operating states of protection element

The behaviour of the protection can be represented using two main discrete states – healthy and pick up states. The continuous states are the voltage (v) and current (i) of the network obtained from instrument transformers. These

are used to determine the network impedance locus (z) as seen at the measurement point. A jump of this continuous state occurs when an in zone fault is introduced into the protected network. The protection then transitions into the 'pick up' discrete state where the protection scheme logic is executed as long as (z) reflects an in-zone fault. The protection scheme logic is mainly the zone timer (and may include protection signalling for communications based distance protection schemes). When the zone timer elapses, a trip command is issued and the continuous state variable resets to a value within the 'healthy' state which reflects the new measured impedance. The trip command is handled by separate logic not illustrated here. Should the fault be cleared before the trip command is issued (e.g. transient fault), then the (z) also resets to the 'healthy' state. For simplicity, additional functions such as power swing blocking, phase selection, etc. are not considered here. But these emphasise the continuous dynamics occurring within a distance protection relay.

Similarly, primary plant controllers (e.g. QB controller) can be represented using a finite state machine with discrete and continuous states. In this case, the QB controller is responsible for adjusting the tap position of the transformer in accordance with a set point that controls the circuit power flow. The tap position control characteristic will be governed by the continuous power flow through the circuit. When certain preconfigured power flow limits are crossed, the controller jumps into a new state represented by a new tap position or even a different operating mode (i.e. boosting, bucking or bypassed). It is then clear the conventional distance protection and QB controllers exhibit both discrete and continuous dynamics. This will be used to model the behaviour of the system in Figure 6-2 using hybrid systems modelling by breaking down the interactions between these elements and associated dynamics. Consequently, the adaptive protection logic will be integrated into the DES abstraction.

Finally, the adaptive protection logic can be similarly broken down into discrete and continuous dynamics. As explained in the previous chapter, the adaptive logic switches between predefined settings groups based on the prevailing power system conditions (i.e. QB state and protection status). The main aspect

of concern in terms of adaptive protection is that of dynamic setting selection. Adaptive protection logic has direct control over the active protection settings by selecting the appropriate setting depending on the primary system conditions that are being monitored. The influence of the active settings on the output of the protection scheme can be described as in (2, 3):

$$Y = f(U, S_n, L) \tag{2}$$

$$U = \dot{X} \cup \Sigma \tag{3}$$

Where Y is the tripping or signaling output of the protection scheme based on the active setting S_n, implemented scheme logic L and scheme input U in the form of measured or derived secondary analogues $\dot{X}$ and/or remote signaling or binary indications Σ. The adaptive protection logic effectively alters the active settings dynamically as in (4):

$$S_n = \delta(U) \tag{4}$$

Where the adaptive protection operator δ acts on the input U to activate the appropriate protection setting S_n. This can simply take the form of a one to one mapping between a subset of $U_n \subseteq 2^U$ and a predetermined settings group $SG \subseteq S_n$.

Table 3 summarises the components of the hybrid system model and the nature of the dynamics exhibited by each. Although different components may serve several functions or exhibit a range of different dynamics, only those of relevance to the development of this hybrid model are listed.

Table 3 Summary of continuous and discrete dynamics in the hybrid system model

Component	Subsystem	Nature of dynamics	Function description/role within the hybrid model
Settings selection logic	Adaptive protection logic	Discrete	Activation of settings group in distance protection IED
Distance protection elements	Distance protection	Continuous	Fault detection according to active settings group
Programmable scheme logic	Distance protection	Discrete	Issue of trip command after elapsed time delay
QB controller	Primary system	Discrete	QB mode and tap position
Transmission circuit	Primary system	Continuous	Line loading status
Transmission circuit breaker	Primary system	Discrete	Line connection status obtained from circuit breaker status

6.4.1.2 Proposed extension of the DES abstraction

In order to understand the interactions between the subsystems further, examine Figure 6-4. This shows a pairing between the different subsystem components and emphasises the relationship between the underlying continuous and discrete dynamics.

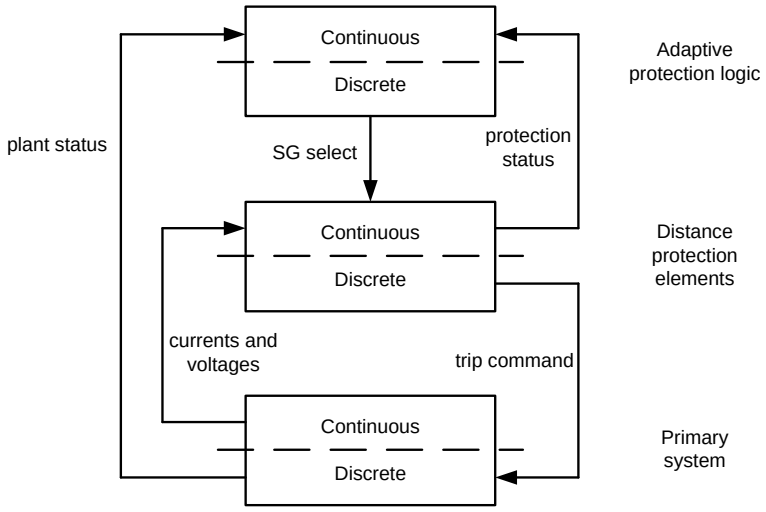

Figure 6-4 Interactions between continuous and discrete components of system under study

The hierarchical control structure provided by the full adaptive protection scheme will be accommodated using two simultaneous DES abstractions as shown in Figure 6-5. Each discrete controller acts on a continuous system. In this case, the conventional distance protection elements act on the primary system in response to a fault condition in a discrete manner (i.e. trip or no trip). Similarly, the adaptive logic reacts to the performance of the conventional protection when triggered by activating discrete protection configurations in the form of a settings group change.

The state variables exchanged follow the same DES abstraction rules set out in the literature described in section 6.2.2. The conventional protection systems will monitor primary system quantities $x_1'(t)$. An event $\tilde{x}_1[n]$ is generated should these quantities exhibit excursions in relation to a certain threshold. For example, the system impedance trajectory seen by the relay enters a distance protection zone. In response, the protection system produces a trip command $\tilde{r}_1[n]$ if the event correlates with the active protection setting. The associated circuit breaker then trips in response to the trip command $r_1(t)$. Similarly, the adaptive protection logic monitors both the states of the protection system $x_2(t)$ and the state of the primary system (or specified components of it) $x_1''(t)$. In this case, these represent the active protection setting and the active QB mode respectively. And changes in the active values of these states triggers the

events $x_2[n]$ and $x_2''[n]$ respectively. The adaptive logic then determines an appropriate setting $\tilde{r}_2[n]$ accordingly and activates it in the target relay by means of $r_2(t)$.

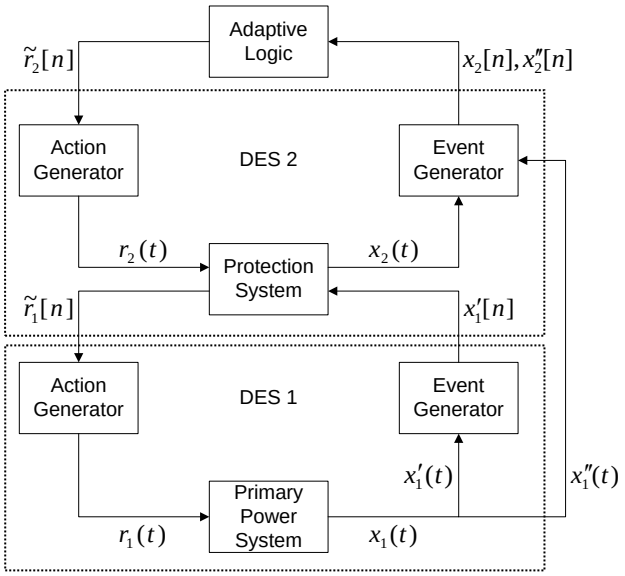

Figure 6-5 DES abstraction representing adaptive protection functionality and its relation to conventional protection elements and the underlying primary system

Now, the newly introduced event and action generators within DES 2 and their associated signals require further development. This will be done with assistance of the developed adaptive distance protection scheme. The events generated are based on the QB status changes and circuit loading conditions. The QB status can be obtained readily from its control indications. Therefore the QB domain Dom_{QB} can be inferred by these status indications. The domain Dom_I of the circuit loading $i(t)$ is bound by $Dom_I(i) = i(t) - i_{enc}(t)$ where $i_{enc}(t)$ is the current which can potentially cause load encroachment. I_{enc} is dependent on circuit configuration and must be determined on a case by case basis. Circuit loading can be a direct result of network topology changes (i.e. loss of parallel circuits), however direct measurement of circuit loading is more accurate than inferring a potential overload from topology information. Protection system state information in the form of an active settings group SG_n is required to reflect the configuration of the protection. Finally, information related to the parallel line connection status is also included through the circuit

breaker status information CB_n. The event generator output $x_2[n]$ is then expressed as:

$$\tilde{x}[n] = \begin{bmatrix} QB_0 & QB_1 & \dots & QB_n \\ I_{enc_0} & I_{enc_1} & \dots & I_{ench_n} \\ SG_0 & SG_1 & \dots & SG_n \\ CB_0 & CB_1 & \dots & CB_n \end{bmatrix} \quad (5)$$

QB_n in the implemented adaptive scheme is defined by the tuple $(QB_{bp}, QB_{bt}, QB_{bk})_n$ for bypass, boost and buck modes respectively, and is obtained directly from the QB substation controller indications. Similarly, CB_n is defined by the pair (CB_{open}, CB_{closed}). The output of the action generator $r_2(t)$ is a signal whose purpose is to activate an appropriate settings group SG_n.

In order to construct the automaton, discrete states, guard conditions and transitions need to be specified. Based on the DES abstraction signal/symbol flows, the primary system automata are shown in Figure 6-6 along with state transition guards.

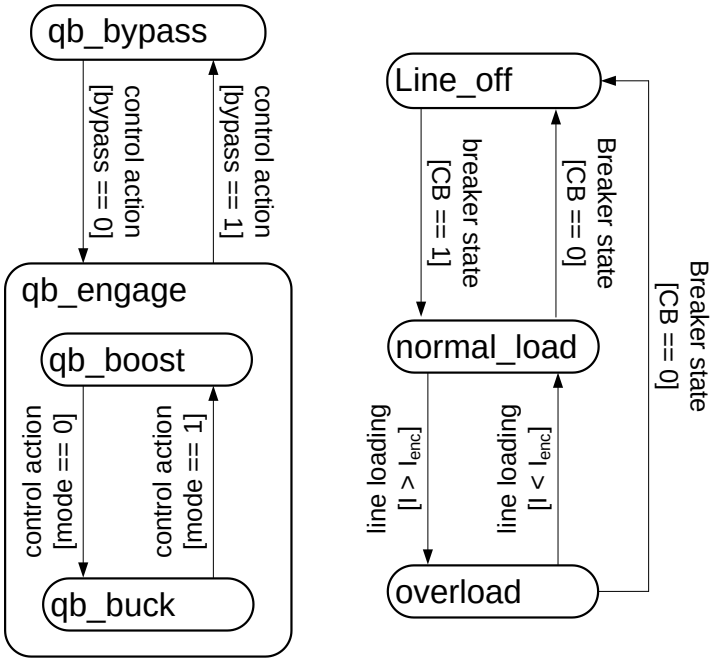

Figure 6-6 Finite automata reflecting primary plant states

6.4.2 Definition of operation and performance states as a prerequisite for reachability analysis

It is proposed that the overall hybrid system is represented using two invariant discrete sets Q_{pps} and Q_{cps} which represent the primary power (pps) system and conventional protection system (cps) respectively. Invariant sets are those where if $x(t) \in Q$ then $x(\tau) \in Q \; \forall \; \tau \geq t$. This applies to all $x(t)$ and $x[n]$ defined in the DES abstraction of Figure 6-5. This means that all primary system continuous states $x_1(t)$ and conventional protection system continuous states $x_2(t)$ are strictly bound by their respective domains $Dom(q_{pps}) \subseteq Q_{pps} \times X_1$ and $Dom(q_{cps}) \subseteq Q_{cps} \times X_2$. Therefore, the discrete states Q_{pps} and Q_{cps} are mutually exclusive. The significance of this will be apparent when the safety property is defined later on. The discrete sets Q_{pps} and Q_{cps} are represented in Figure 6-7. It can be seen that Q_{pps} represents the different primary system states related to the operation of the primary system (specifically QB operation). Also, Q_{cps} reflects the different operational modes of a conventional protection relay as dictated by its settings. Q_{pps} and Q_{cps} will thereafter be referred to as 'operational states'. Discrete transitions between the sub-states $q_{pps} \subseteq Q_{pps}$ and $q_{cps} \subseteq Q_{cps}$ are indicated by T. These sub-states must also be, by definition, mutually exclusive to facilitate the definition of safe state.

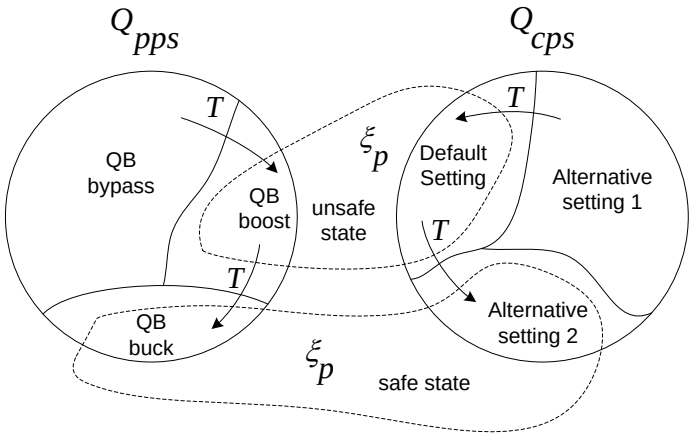

Figure 6-7 Partitioning of the hybrid state space

In addition to the operational states, it is now proposed that new invariant discrete sets $\xi_p$are created and called 'performance states'. These performance

states represent unique groupings of operational sub-states. In other words, no two sub-states belonging to an operational state share the same performance state grouping. For instance, the performance state that groups 'QB buck' and 'Alternative setting 2' sub-states shall not include 'Default setting' or 'QB bypass' under the same grouping.

6.5 Reachability analysis for the verification of the developed adaptive distance protection logic

The analysis focuses on the erroneous adaptive protection behaviour caused by an unsatisfactory response of the dynamic setting selection function in response to a primary system stimulus. To this end, reachability analysis is proposed to examine the possibility of reaching an undesired response. This property is hereafter referred to as the safety of the adaptive protection logic. One of the key requirements of conducting reachability analysis is defining the unsafe states that the system must not reach or dwell in. Given that the adaptive logic may take a finite time to determine the appropriate setting, dwelling in an unsafe state may be acceptable. This is the case given that a maximum time delay for the unsafe state exit transition is specified. Note that it was shown experimentally in chapter 5 that the implementation of the scheme has an impact on this time delay which can be variable. Nevertheless, it is important to determine the acceptable boundaries for this delay. Therefore, verifying this condition in the adaptive protection scheme context requires the examination of unsafe states entry and exit during the adaptive logic operation.

The performance invariant sets ξ_p previously defined are used to identify these unsafe states $\overline{G} \subseteq \xi_p$. Where $\overline{G}$ denotes an unsafe state. In Figure 6-7, the performance state combining the 'default setting' and 'QB boost' states is considered unsafe since this particular combination results in distance protection under reach. As mentioned previously, invariant sets are mutually exclusive. Thus, the boundaries of the performance states can be clearly defined in the hybrid state space. Ultimately, this will result in a clear (binary) indication of whether a particular state can be considered safe or not.

The system should either never exist in an unsafe state $\overline{G}$, expressed as:

$$\square((q, x) \notin \overline{G}) \tag{8}$$

Where $\square$ is the 'always' logical operator, or alternatively, the system should eventually always exit the unsafe state:

$$\Diamond\square((q, x) \notin \overline{G}) \tag{9}$$

Where $\Diamond$ is the 'eventually' logical operator. This temporal aspect reflects the finite amount of time required to exit an unsafe state through adaptive protection setting changes. To formally examine the temporal dimension from a hybrid system perspective, timed hybrid automata can be considered. However, this is out of the scope of the thesis.

The backwards trajectory obtained from the unsafe transition $T_{\overline{G}}$ can be used to identify faults in the adaptive logic, by observing the scheme inputs and the resulting adaptive logic state transitions leading to the unsafe state entry. In light of this, a safety performance verification procedure based on reachability analysis is proposed and is shown in Figure 6-8. This will be used on the adaptive distance protection scheme previously developed. While conducting the reachability analysis as outlined in Figure 6-8, it is important to stimulate the system with inputs for each set of initial conditions. It is worth noting in this case, that merely residing in an unsafe state does not necessarily reflect that the system under test is unsafe. Since the adaptive protection logic takes a finite amount of time to respond to changes in the network, this should always be taken into account in the analysis.

The dotted region within Figure 6-8 indicates the use of Q_{pps}, Q_{cps} and ξ_p defined earlier. The unsafe states are mapped directly to these invariant sets as will be reflected in the implementation below.

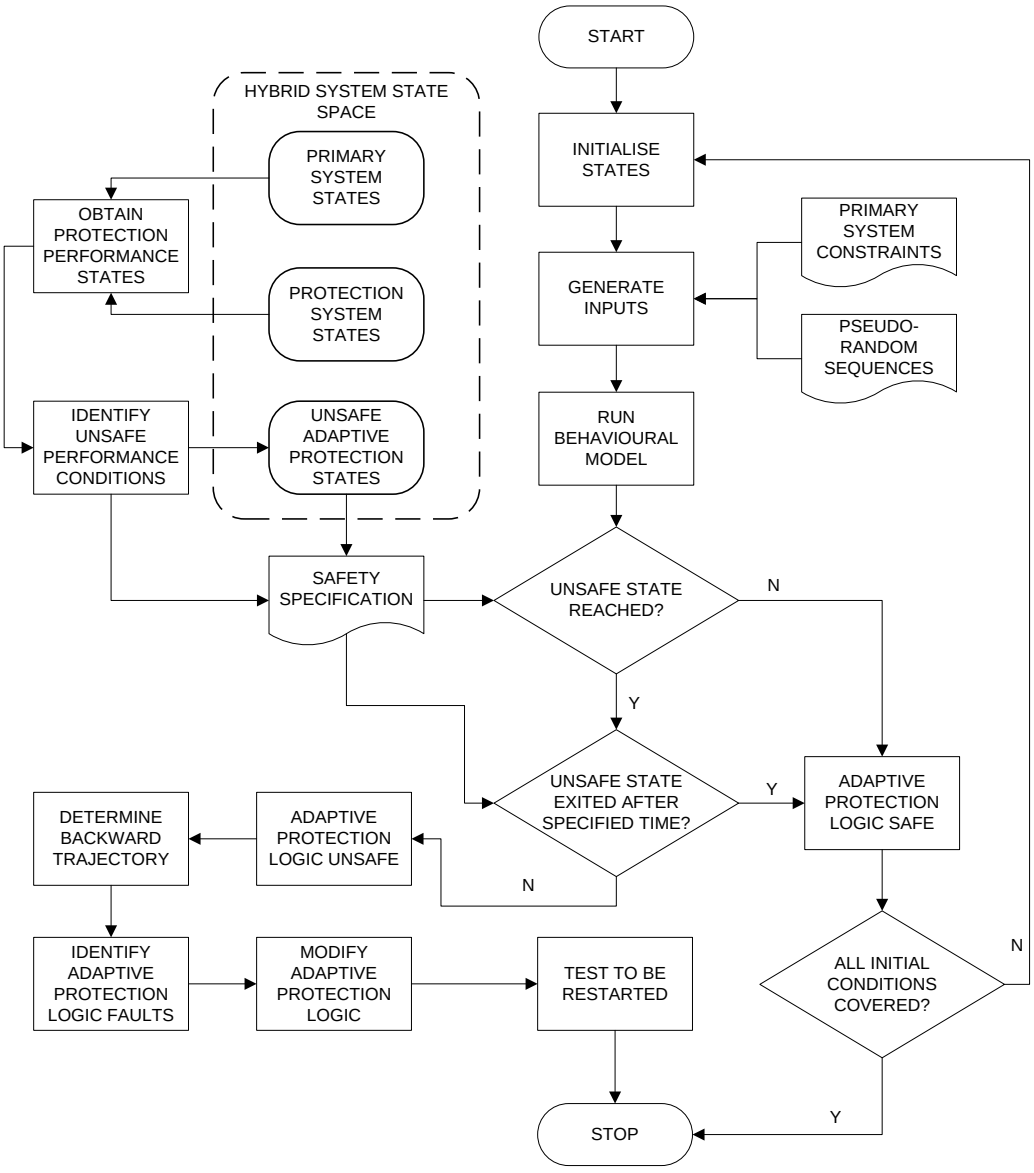

Figure 6-8 Reachability analysis procedure

6.5.1 Reachability verification implementation in Simulink

Simulink Stateflow was used in order to implement the reachability analysis on the adaptive distance logic which was also developed in Simulink as described in chapter 5. A state monitor was created to identify the state the system resides in at any given time. This is connected to the outputs of the adaptive protection algorithm developed in chapter 5 and is illustrated in Figure 6-9 (the connection between the different Simulink subsystems can be observed in Appendix B). The states defined in the Stateflow charts reflect the operational and performance states defined earlier.

The inputs to the state monitor are:

- The reach error which identifies whether the distance relay is over-reaching, under-reaching or at nominal reach.
- The line loading which is a binary signal representing the loading condition of the protected transmission line. Should the load exceed a pre-set threshold, the value of the signal is set and vice versa.
- The active settings group.
- The remote extension blocking signal which prevents zone extension to avoid zone 2 mis-coordination with adjacent lines.

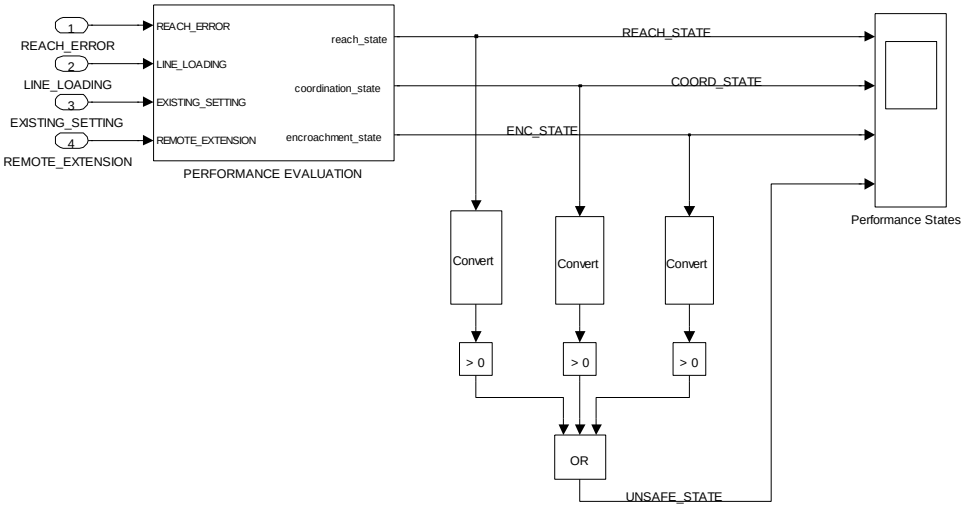

Figure 6-9 Reachability analysis subsystem

The outputs of the reachability analysis subsystem are three enumerated signals described in the boxes below. The enumeration simplifies the reading of the outputs. These signals are the 'Performance Reach States', 'Performance Encroachment States' and 'Performance Coordination States'. These signify the occurrence of reach errors, potential load encroachment or mis-coordination respectively – mal operation conditions described in chapter 4 and will be tested for later on. The occurrence of any enumerated value other than '0' means that an unsafe state has been reached. An additional derived output (Unsafe State) is used to quickly identify reaching an unsafe state through using a logical OR gate. The Stateflow charts within the reachability analysis subsystem are shown in Figure 6-10. Each of the charts is responsible for identifying whether the adaptive protection scheme resides in an unsafe state.

```
classdef(Enumeration) PerformanceReachStates < Simulink.IntEnumType
  enumeration
    NORMAL_REACH(0)
    OVER_REACH(1)
    UNDER_REACH(2)
  end
end

classdef(Enumeration) PerformanceEncroachmentStates <
Simulink.IntEnumType
  enumeration
    NO_ENCROACHMENT(0)
    ENCROACHMENT_POSSIBLE(1)
  end
end

classdef(Enumeration) PerformanceCoordinationStates <
Simulink.IntEnumType
  enumeration
    COORDINATED(0)
    MIS_COORDINATION(1)
  end
end
```

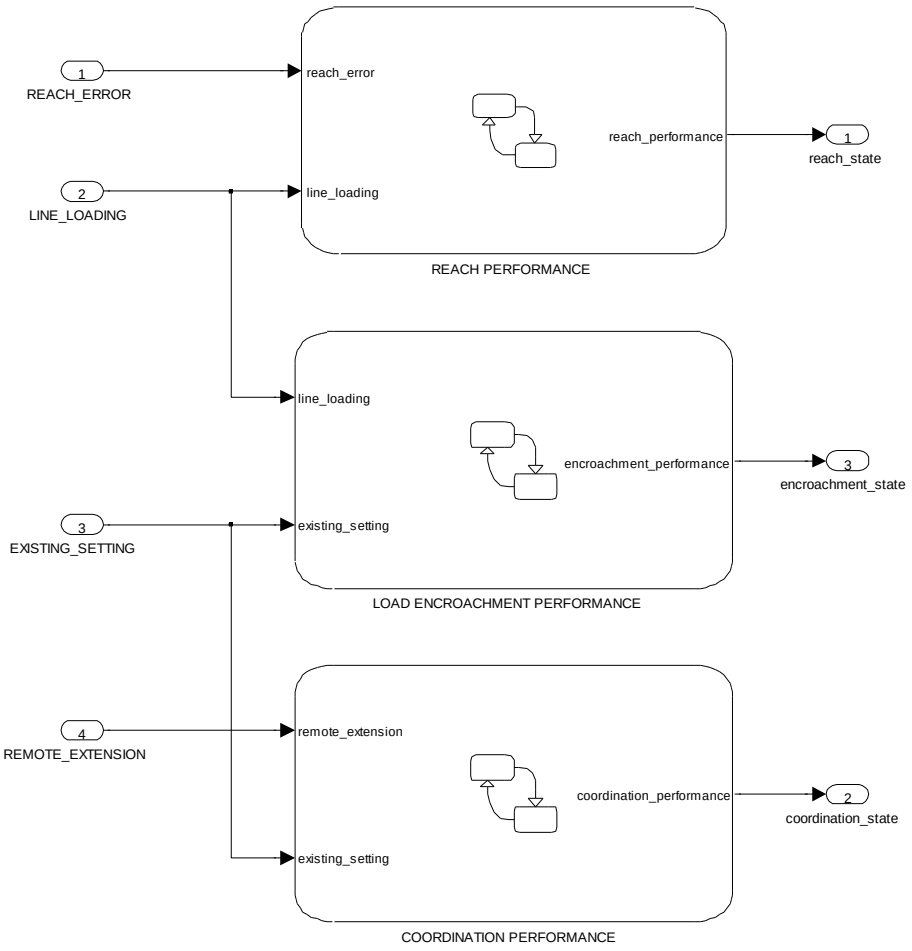

Figure 6-10 Stateflow subsystem for reachability analysis showing three categories under test

The automaton for the first chart responsible for determining that a zone reach unsafe state has been reached is shown in Figure 6-11. Transition guard conditions rely on the adaptive algorithm reach error signal and line loading conditions.

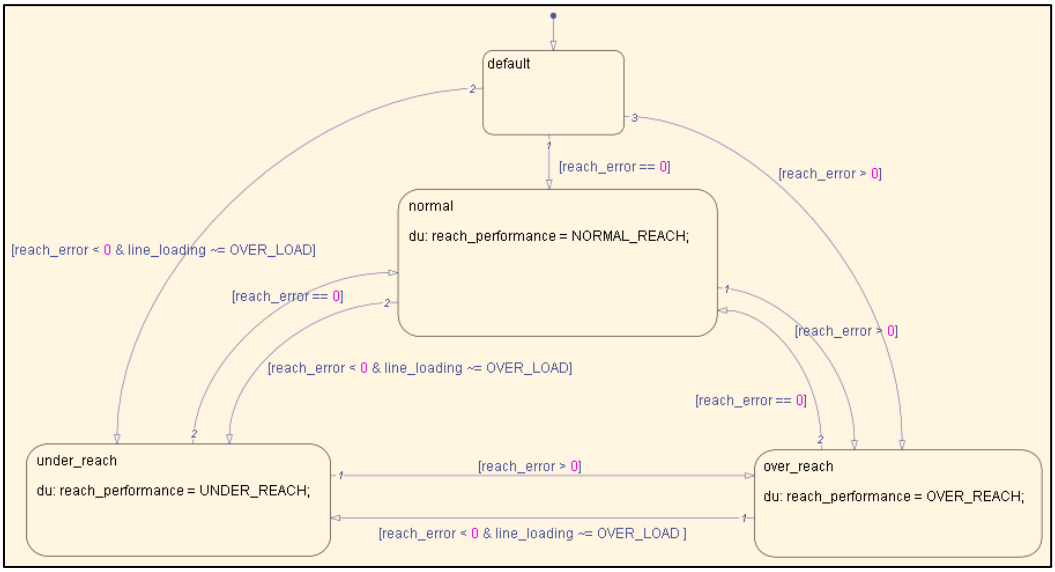

Figure 6-11 Reach performance Stateflow state diagram (automaton)

Figure 6-12 shows the automaton responsible for determining whether the potential for reaching a load encroachment state is possible due to zone reach extension couple with line overload. The transition guard conditions in this case rely on the active settings group and the line loading condition.

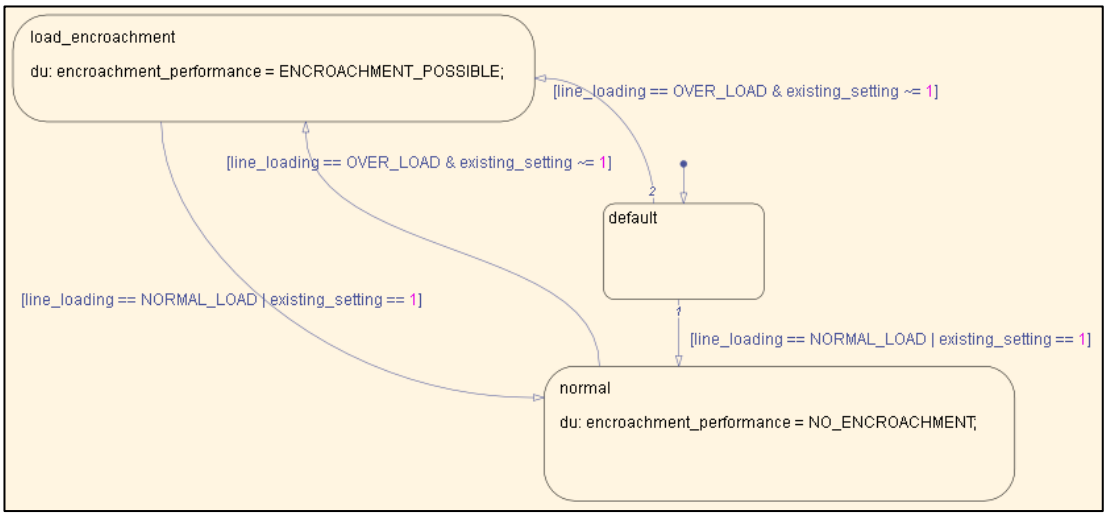

Figure 6-12 Load encroachment performance Stateflow state diagram

Finally, reaching a zone 2 mis-coordination state is determined in the automaton shown in Figure 6-13. The transition guard conditions rely on the active settings group and the value of the zone extension blocking signal.

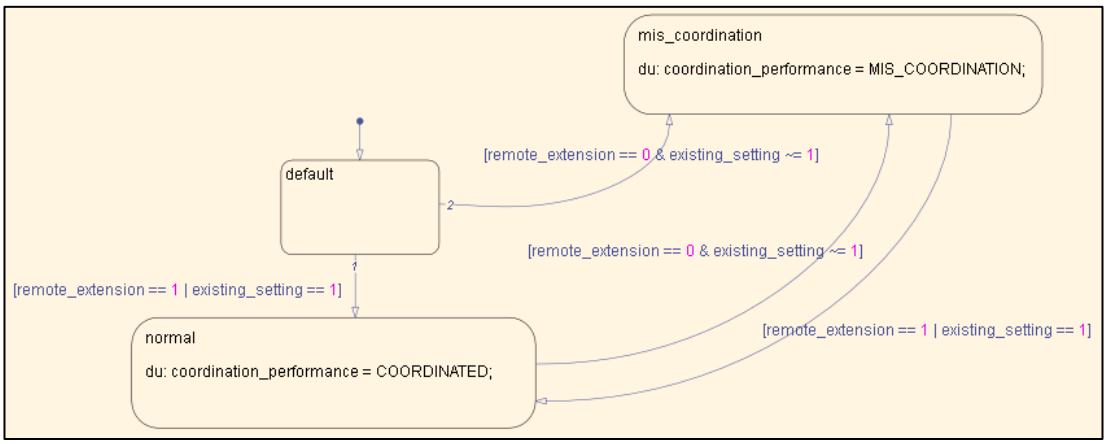

Figure 6-13 Adjacent line coordination performance Stateflow diagram

6.5.2 Reachability analysis test setup and results

As mentioned earlier, the reachability analysis subsystem is connected to key signals from the adaptive protection logic developed in Simulink as shown in Figure 6-14. The outputs from the analysis block are directly observed using the available scope and can be stored for offline analysis. The inputs to the system are QB status indications represented using a PRBS obtained from the Simulink signal builder. A pseudo-random binary sequence (PRBS) was used for this purpose as it is considered an effective means of providing exhaustive coverage for possible system executions [17]. The PRBS used is shown in Figure 6-15 and the simulation was run for 50s to exhaustively test the algorithm.

Circuit breaker status information were also synthesised using the signal builder. Circuit breaker information is used to determine whether a short adjacent line is active. If this condition is identified and the distance zone has been extended, then a zone 2 mis-coordination may occur. The line loading signal was a threshold value based in a simulation detailed in Appendix C which represents the upper loading limit of the protected circuit prior to potential load encroachment. This is appropriate since the primary system model is absent from the analysis as mentioned before.

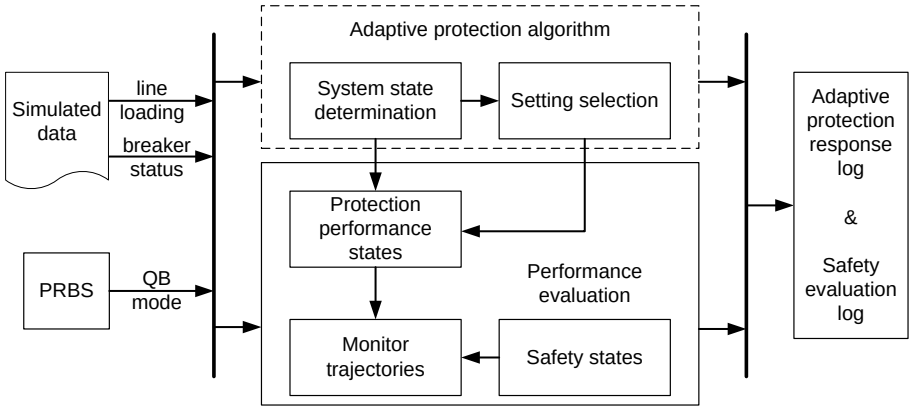

Figure 6-14 Structure of the Simulink test harness for performing reachability analysis

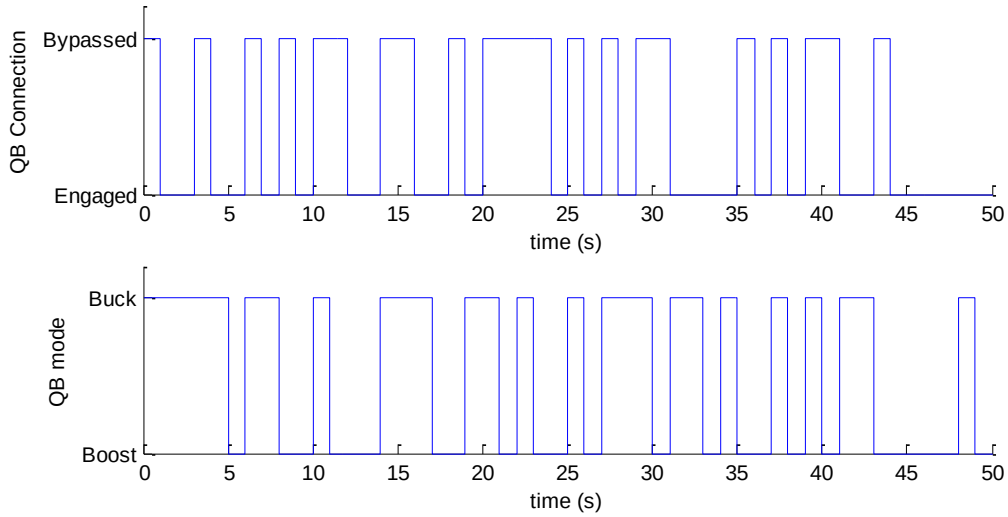

Figure 6-15 QB states for stimulating the adaptive protection logic using a PRBS

The unsafe state, their state transition conditions according to the DES abstraction and the unsafe state exit conditions are shown in Table 4. The ' $\overline{\ }$ ' operator indicates the complement of the state. Note that SG2 is not used as discussed chapter 4 and 5.

Table 4 Safety conditions for adaptive logic under test

$\overline{G}$	$x_2''[n], x_2[n]$	$T_{\overline{G}}$ Exit Conditions
Under-reach	QB_{bk}, SG_1	$QB_{bp} \vert SG_3$
Under-reach	QB_{bt}, SG_1	$QB_{bp} \vert SG_4$
Over-reach	QB_{bp}, SG_1	$QB_{bt} \vert QB_{bk} \vert SG_1$
Load-encroachment	$I_{enc}, \overline{SG_1}$	$\overline{I}_{enc} \vert SG_1$

Figure 6-16 shows the outputs from the reachability analysis subsystem in response to the inputs previously described. The active settings groups are also shown. The safety states trace indicates that unsafe states have been reached a number of times. These occurrences reflect the reach errors shown in the figure. This can be explained by the finite amount of time the adaptive logic takes to determine change settings when the QB state changes. Due to the short simulation time step used (1ms), the logic only resides in the unsafe state for a maximum of 1ms. In reality, this may take several cycles or as shown in chapter 5, several seconds depending on the algorithm implementation.

After 25s of simulation time, the inputs current is increased to cross the threshold such that the potential for load encroachment arises. In this case, the adaptive protection logic reverts to the default settings group (SG1) and does not attempt to extend the reach of the protective zones regardless of the QB mode. Consequently no reach errors occur during these mode changes. This condition can be observed in the automaton of Figure 6-12.

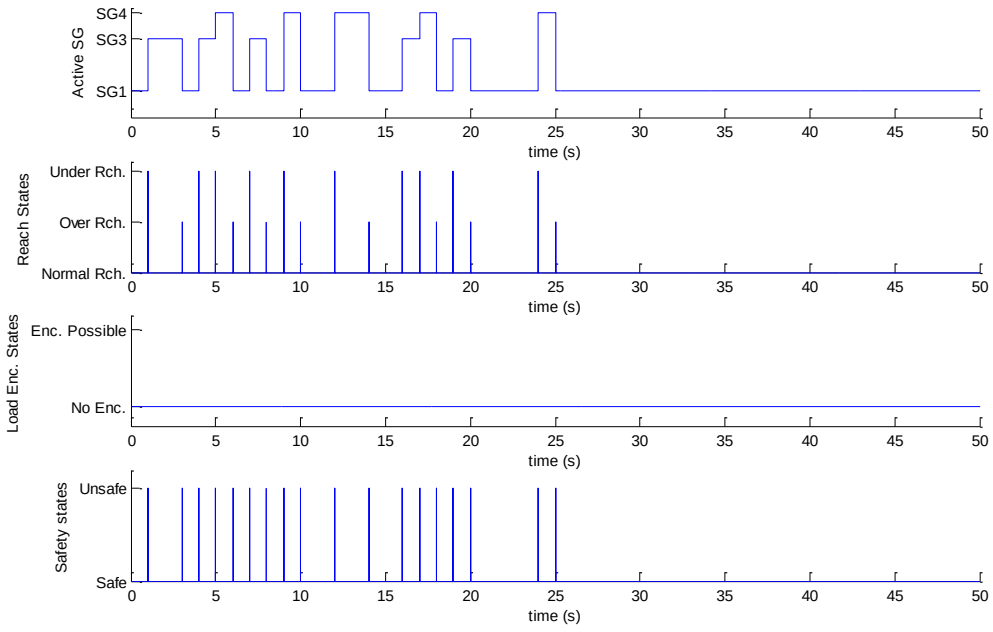

Figure 6-16 Correct operation of adaptive logic indicated by safe states

To further test the reachability analysis implementation. A fault was introduced in the adaptive logic. The ability to block zone reach extensions during line overloads (potential load encroachment) was disabled and the same inputs as in the previous case were applied.

It can be seen in Figure 6-17, that the reachability analysis has indicated that the system reached unsafe states on several occasions after 25s of simulation. Zone extension was sanctioned on several occasions due to QB mode changes when it should have been blocked due to line overload. It can also be seen that the logic dwells in these states for longer that 1ms (simulation time step). Thus, the logic in this case is indeed unsafe.

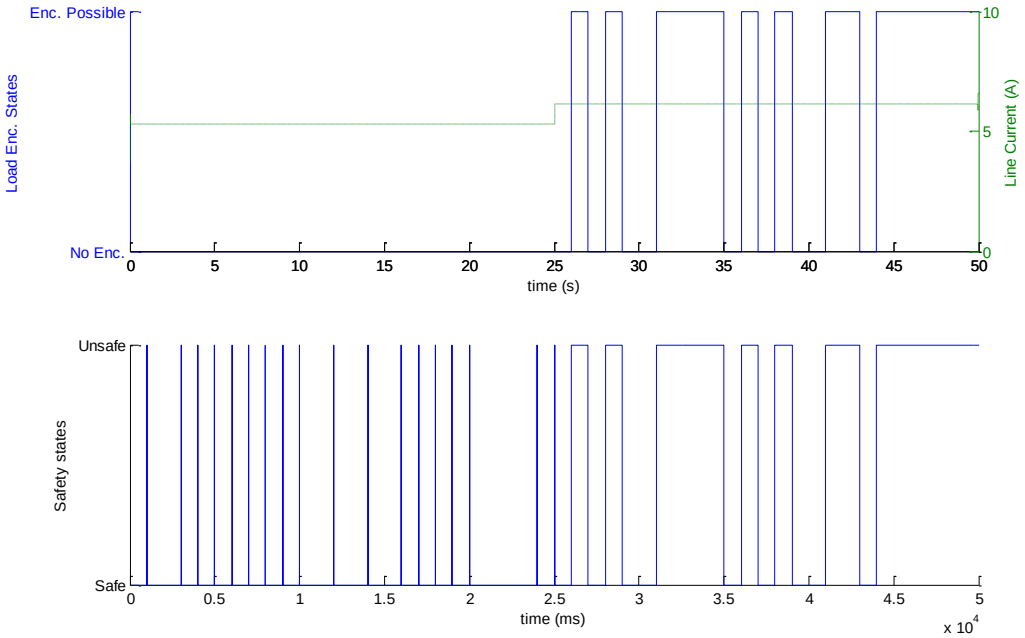

Figure 6-17 Failure of adaptive logic leading to unsafe state detection

6.6 Discussion of reachability results and the role of formal approaches to the verification of adaptive protection functionality

So long as the power system state can be inferred from a set of discrete transitions, then explicit continuous space computations will not be necessary. However, this assumes that the evolution of the continuous primary system state is not influenced by the outcome of the logic decision. Given the scope of the verification, this assumption is valid. This is because the verification is being conducted to determine whether logic actions are safe based on the consequences of an unsafe outcome. And these unsafe outcomes have been determined using the performance states ξ_p. The temporal dimension of the reachability analysis is also of relevance to this matter. It is necessary to identify the maximum time period that an adaptive protection scheme requires to provide a decision. Otherwise the adaptive scheme may become vulnerable to mal-operation if changes in the primary system occur during this time period. Therefore, further work is necessary to incorporate the temporal dimension into the hybrid model and consequent reachability analysis.

The practical utilisation of the safety verification would be of interest to manufacturers and utilities dealing with adaptive protection. Although protection scheme developers can directly apply such verification methodologies on their adaptive algorithms, utility commissioning engineers require meaningful performance metrics without delving into the intricacies of system behavioural modelling. As such, it is important to migrate such methodologies into tools and processes that meet usability requirements of end users.

The role of formal verification approaches should be complementary to simulation methods such as hardware in the loop testing as presented in the previous chapter. The challenge lies in striking an effective balance between the two approaches. Simulation based methods' shortcomings become apparent when there is no traceability between the system requirements, the test cases

(inspired by scheme use cases). As such it becomes more difficult to explore the full extent of the scheme performance or envisage conditions not defined by the original test scenarios and indeed usage scenarios. In other words, simulation based testing can only be as comprehensive as the designed for operating conditions. Furthermore, as adaptive protection functions are applied to perform wide area functions, the process of simulation based testing becomes more difficult due to requirements for developing larger network models and the need for multiple adaptive protection devices integrated over a communications network. Furthermore, commissioning testing of such scheme becomes more difficult due to the physically expansive nature of such schemes and the limitations in obtaining substation outages. Thus, more emphasis can be placed on more formal testing approaches to offset these limitations.

6.7 Chapter summary

This chapter presented a formal method verifying the safety property of an adaptive protection scheme logic based on reachability analysis. This required modelling the scheme's behaviour in a hybrid systems paradigm. To achieve this, the chapter established the minimum level of discrete abstraction of the state space of the system under test. The abstraction was necessarily extended, compared to previously proposed representations, to cater for the additional control loop that the adaptive logic introduces. This was followed by devising a reachability analysis procedure which makes use of the developed abstraction. Furthermore, the state space of the system under test was broken down into a group of invariant sets that represent operational and performance modes of the primary system and underlying protection scheme. Related state transitions were inferred without the need for computing continuous field vector within each state. This means that in this case, computational resources are not a limiting factor to conducting the analysis.

The effectiveness of the reachability analysis in identifying potentially unsafe adaptive logic operation was demonstrated using an example adaptive distance

protection scheme. Finite time required to select between different settings, both in simulation and in real world deployments, meant that a temporal dimension must be considered during the safety assessment. The logic can only be deemed unsafe if it dwells (rather than enters) an unsafe state for specified period of time depending on the application. The reachability analysis provided easy to interpret safety indications when the scheme under test was subjected to a number of different inputs representing a range of operational circumstances it may be subjected to.

6.8 References

[1] X. D. Koutsoukos, P. J. Antsaklis, J. A. Stiver, and M. D. Lemmon, "Supervisory control of hybrid systems," *Proceedings of the IEEE,* vol. 88, pp. 1026-1049, 2000.

[2] E. M. Navarro-López and R. Carter, "Hybrid automata: an insight into the discrete abstraction of discontinuous systems," *International Journal of Systems Science,* pp. 1-16, 2010.

[3] Y. Susuki, T. J. Koo, H. Ebina, T. Yamazaki, T. Ochi, T. Uemura*, et al.*, "A Hybrid System Approach to the Analysis and Design of Power Grid Dynamic Performance," *Proceedings of the IEEE,* vol. 100, pp. 225-239, 2012.

[4] C. J. Tomlin, I. Mitchell, A. M. Bayen, and M. Oishi, "Computational techniques for the verification of hybrid systems," *Proceedings of the IEEE,* vol. 91, pp. 986-1001, 2003.

[5] Y. Susuki, T. Sakiyama, T. Ochi, T. Uemura, and T. Hikihara, "Verifying fault release control of power system via hybrid system reachability," in *Power Symposium, 2008. NAPS '08. 40th North American*, 2008, pp. 1-6.

[6] G. K. Fourlas, K. J. Kyriakopoulos, and C. D. Vournas, "Hybrid systems modeling for power systems," *Circuits and Systems Magazine, IEEE,* vol. 4, pp. 16-23, 2004.

[7] Y. Susuki and T. Hikihara, "Predicting Voltage Instability of Power System via Hybrid System Reachability Analysis," in *American Control Conference, 2007. ACC '07*, 2007, pp. 4166-4171.

[8] G. K. Fourlas, K. J. Kyriakopoulos, and N. J. Krikelis, "Fault Diagnosis of Hybrid Systems," in *Intelligent Control, 2005. Proceedings of the 2005 IEEE International Symposium on, Mediterrean Conference on Control and Automation*, 2005, pp. 832-837.

[9] G. K. Fourlas, "An approach towards fault tolerant hybrid control systems," in *Control & Automation, 2007. MED '07. Mediterranean Conference on*, 2007, pp. 1-6.

[10] G. K. Fourlas, "Modeling of an electrical power transmission system using hybrid systems," in *Control Applications, 2005. CCA 2005. Proceedings of 2005 IEEE Conference on*, 2005, pp. 1516-1521.

[11] I. A. Hiskens and M. A. Pai, "Hybrid systems view of power system modelling," in *Circuits and Systems, 2000. Proceedings. ISCAS 2000 Geneva. The 2000 IEEE International Symposium on*, 2000, pp. 228-231 vol.2.

[12] M. Yasar, A. Beytin, G. Bajpai, and H. G. Kwatny, "Integrated Electric Power System supervision for reconfiguration and damage mitigation," in *IEEE Electric Ship Technologies Symposium, 2009. ESTS 2009*, 2009, pp. 345-352.

[13] M. Lindahl, P. Pettersson, and W. Yi, "Formal design and analysis of a gear controller," *International Journal on Software Tools for Technology Transfer (STTT),* vol. 3, pp. 353-368, 2001.

[14] R. Goebel, R. Sanfelice, and A. Teel, "Hybrid dynamical systems," *Control Systems Magazine, IEEE,* vol. 29, pp. 28-93, 2009.

[15] H. Guéguen, M.-A. Lefebvre, J. Zaytoon, and O. Nasri, "Safety verification and reachability analysis for hybrid systems," *Annual Reviews in Control,* vol. 33, pp. 25-36, 2009.

[16] R. R. Negenborn, A. G. Beccuti, T. Demiray, S. Leirens, G. Damm, B. De Schutter*, et al.*, "Supervisory hybrid model predictive control for voltage stability of power networks," in *American Control Conference, 2007. ACC '07*, 2007, pp. 5444-5449.

[17] M. G. Bartley, D. Galpin, and T. Blackmore, "A comparison of three verification techniques," 2002.

7 Thesis Conclusions and Future Work

7.1 Qualitative reflection on the general hypothesis

It has been shown through extensive simulations and critical literature review that an adaptive protection philosophy plays an important role in improving the performance of protection under flexible power system operating conditions. It has been shown that only through rigorous scheme modelling and comprehensive testing methodologies that well engineered (designed, implemented and tested) adaptive protection schemes can be integrated into the power system to perform their safety critical functions in a satisfactory manner with greater flexibility compared to a conventional protection philosophy.

7.2 Evaluation of conventional protection performance

The performance of distance protection for transmission circuits with quadrature booster (QB) transformers has been quantified under varied QB operating conditions and fault conditions for the first time. The distance protection can under-reach with increased tap position. Simulations have shown a maximum measured impedance error of 3.53Ω (75%) and 5.68Ω (64%) for boost and buck modes respectively (expressed in secondary ohms). The under reach only occurs for unsymmetrical faults and the maximum error occurs for phase to phase faults. The inherent impedance of the QB results in an additional offset in terms of the impedance error. Due to the coverage of the MHO characteristic, under reach for non-resistive faults only becomes an issue at around 7° and 15° phase shift for zone 2 and zone 3 respectively. Zone 1 is unaffected due to the position of instrument transformers – downstream of the QB. The protection has the potential to over-reach by up to 0.15pu (assuming typical QB impedance) if the QB is bypassed while backup protection zones

(zones 2 and 3) are set to ensure protection of the remote bus bar. This is usually mitigated by applying more conservative reach settings for back up protection zones.

Operating a collection of QBs in a coordinated control strategy, as planned by National Grid, has no additional effect on the reach errors from an individual distance protection relay's point of view. This has been verified by operating QBs in parallel in circuits with close proximity based on a section of the National Grid transmission network. However, static reach settings based on the operating ranges of QB may not always be valid for such a coordinated control strategy. This is because of the potential for QBs to alter their operating modes more regularly and operate at tap positions that the system operator may not have envisaged particular QBs operating at.

The performance of loss of mains protection functions (ROCOF) has been quantified for different generator technologies and for different manufacturer implementations of these functions through extensive secondary injection testing. The testing showed some inadequacy of settings recommended by engineering recommendations ER G59/2 especially for ensuring loss of mains protection stability against remote disturbances. This is especially true for inverter-interfaced generators which require in some cases desensitising the ROCOF protection to 3Hz/s, rendering it ineffective for true loss of mains conditions. Thus ROCOF should not be used with such generators where simple under/over voltage and frequency protection would perform better under loss of mains situations.

For a given ROCOF setting, the testing also showed that there was disparity in the performance between different manufacturer relays which is attributed to different methods in measuring frequency. Without stipulating minimum performance requirements for the frequency measurement algorithms, it would be difficult to ensure repeatability in performance across a wide range of manufacturer solutions.

7.3 Design of adaptive protection schemes

It was shown that one of the most important design decisions made in developing an adaptive protection scheme (from the point of view of scheme verification), is the amount of flexibility that should be introduced by the scheme functionality. This manifested itself in the approach to choosing the active protection setting. Choosing active protection settings from a limited pool of pre-calculated settings groups is more desirable from a scheme validation point as opposed to using online settings calculations. The number of settings groups necessary is highly dependent on the protection scheme and application. Generally speaking, the trade-off between the simplicity and flexibility provided by a limited or large number of settings groups respectively is determined by the increase in risk of continuous settings changes due to a higher resolution provided by a larger number of settings groups and the additional risk of scheme failure because of this. Moreover, the more settings groups used, the less distinct the approach becomes compared to online calculations, which diminishes its validation advantage.

The adaptive distance protection scheme developed in this thesis was limited by the maximum number of settings groups provided by the relaying platform – four in this case. Theoretically however, this can be expanded to provide a dedicated settings group for each mode of the QB and associated tap positions – that is up to 41 settings groups for a typical QB. The effort in validating this amount of settings groups becomes magnified, where in reality adjusting distance zone reach is always governed by error margins of about +/-5% of reach setting based on engineering practices and testing standards. Thus, a theoretical upper limit of settings groups can be applied based on this error margin. In this particular case, 10 settings groups have been shown to be sufficient.

The operational scope of adaptive protection functionality was defined, for the first time in this thesis, to ensure valid performance at the design stage. This was achieved by designating the roles of adaptive and conventional functions. It was shown that adaptive protection functions are more suited to performing

tasks triggered by non-fault events such as system reconfiguration. Conversely, tasks performed during a fault transient should be preserved for conventional protection functions that have been configured by adaptive functionality beforehand – again appropriately when triggered.

7.4 Structural and behavioural modelling of adaptive protection schemes

The concept of an adaptive protection architecture (APA) was further developed through the definition of minimum functional elements and interfaces for each of its layers. This has been shown to achieve, for the first time, the following:

- Ensured the architecture's applicability to transmission level adaptive protection applications and consequently a wider application domain than the original conceived conceptual applications.
- Enabled the implementation and experimental testing of an adaptive protection scheme (adaptive distance protection developed in the thesis) based on the architecture.
- Facilitated adaptive scheme validation by providing a reference functional and performance specification that is independent of the scheme implementation.

Furthermore, this development of the architecture concept enabled creating a clear distinction between what constitutes coordination and management layer functions. This distinction has been shown to be based on three criteria – the nature of information used to infer system state, protection operation time frames and the breadth of protection actions each layer exerts on another.

To facilitate the performance verification of adaptive protection algorithms, a novel approach based on hybrid systems was used to describe its behaviour – that is a characterisation of its response to measured events in the protected system. The application of hybrid systems modelling to adaptive protection schemes is the first of its kind.

It has been shown that standard approaches to abstracting the behaviour of hybrid systems (discrete event system abstractions) had limitations in encompassing the hierarchical 'control' nature of adaptive protection based on the APA. The work reported in this thesis has been shown to overcome this limitation by extending the definition of these behaviour abstractions. This necessarily required the definition of additional interfaces and interactions between constituent elements of the behaviour model.

7.5 Validation and verification of adaptive protection schemes

The adaptive distance protection scheme developed and implemented in this thesis was shown, using hardware in the loop validation, to provide an improvement in selective reach of up to 20% of protected line impedance for zone 2 – an improvement limited by coordination with adjacent line protection zones. Thus, performance of backup protection is restored dynamically based on the state of the QB transformer and circuit being protected.

The functional abstraction of the APA enabled performing unit testing of constituent components of the developed adaptive distance scheme as well as the validation of the overall scheme more effectively. This is due to the ability to define more clearly the functional and non-functional requirements for the adaptive schemes components and the expected overall scheme performance under varied operating conditions of the QB transformer. In other words the scheme requirements were more traceable and as such more confidence can be obtained from the adaptive scheme validation process.

This thesis reported the first application of reachability analysis (based on the hybrid behavioural model) as a means of verifying the performance of adaptive protection schemes. The reachability analysis methodology presented in this thesis was demonstrated through verifying the safety property of the adaptive settings selection logic for the developed distance protection scheme. The reachability analysis methodology reported in this thesis is also novel in the approach to defining the boundaries of the reachable state space representing unsafe adaptive performance.

It has been demonstrated that the approach to defining the unsafe state space eliminated the need for explicitly computing the continuous state space of the underlying hybrid behavioural model provided that:

- The continuous evolution of the primary system states are not directly influenced by the outcome of the adaptive setting selection logic.
- The adaptive logic forms part of the coordination layer functionality.

As such efficiencies in the verification process are gained. The approach to defining the state space is based on splitting the hybrid system state space into 'operational' and 'performance' invariant sets through which a direct mapping between power system conditions and scheme performance can be made. This process necessitated defining the state transitions (and guard conditions) associated with these invariant sets.

The adaptive scheme verification through reachability analysis has been shown to incorporate a temporal aspect that reflects the adaptive scheme's finite response time to changes in the power system. Design and implementation measures can be put in place to minimise this time delay. The required improvements in the time response are dictated by the acceptable duration of power system vulnerability caused by the temporary degradation of protection performance levels. To better characterise this temporal aspect, it is then necessary to use timed automata to model the hybrid state space.

Testing adaptive protection schemes must generally incorporate the full complement of simulation and formal testing methods. This is necessary to address inherent limitations of simulation based testing stemming from the design of the testing scenarios. Therefore, testing approaches stipulated by testing standards still hold but should be extended with approaches developed in the thesis to incorporate the characteristics of interactions between conventional and adaptive functions. More emphasis should be placed on formal testing as it becomes more difficult to test the full set of potential operating scenarios in the field during scheme commissioning – a task that is even more difficult when the schemes perform wide area protection functions.

7.6 Future work

Interfaces and functions within the adaptive protection architecture have been defined. However, this can be taken a step further by using standard ways of describing and implementing the architecture. For instance, IEC 61499 event driven function blocks can be used to represent the architecture's constituent functions as standard executable elements. The use of standard interfaces simplifies the process of porting these functions into different platforms. Further research is necessary to determine methods of distributing adaptive functionality. And the use of IEC 61499 enables such an approach as it supports describing distributed control functionality.

A full suite of formal performance verification techniques can be applied with the aid of the behavioural model. These include determinism and observability. Knowledge of the current state of the adaptive logic and stimulating inputs, results in knowledge of its output if it is deterministic. Also, the state of the adaptive scheme can be identified by observing its inputs and outputs in relation to the behavioural model. The significance of determining these properties lies in offering complementary methods that can be used to verify the adaptive protection functions' performance.

Making full use of management layer functions necessitates identifying system integrity protection schemes (SIPS) that would benefit from adaptation in their performance. Moreover, techniques of establishing the system state and its impact on system protection performance must be developed. Changing the configuration of system protection, in this case, requires greater levels of coordination to avoid conflict in performance objectives between coexisting system protection schemes. The developed hybrid system model will prove to be a powerful approach to understanding this complex problem and reachability analysis is one of the tools that should be used to determine the safety of these interactions.

Appendix A Test transmission network model data and protection settings

Table A-1 details the transmission network model substation data in terms of voltage, fault level and derived source impedance (Z_s). This is obtained from the NG seven year statement for 2010/2011. The parameters of the distance protection model are summarised in Table A-2 and Table A-3. Finally, the transmission network line data is detailed in Table A-4. This data was also obtained from the NG seven year statement, apart from zero sequence parameters where typical values were used.

Table A-1 Substation data for test transmission network

Substation	Voltage (kV)	Fault level (kA)	X/R	Z_s (Ω)	$<Z_s$(°)
RATS	400	38.52	12	5.9953	85.24
WBUR	400	39.66	12	5.823	85.24
HIGM	400	30.8	12	7.4981	85.24
GREN	400	31.64	12	7.299	85.24
WILE	400	38.22	12	6.0424	85.24
STAY	400	28	12	8.2479	85.24
COTT	400	46.22	12	4.9965	85.24

Table A-2 Distance relay model configuration and related data

Protection parameters	Configuration
RCA	84.67°
k_0 calculation	Automatic
CT ratio	1000/1 A
CVT ratio	400kV/110V
Tripping	3 pole

Table A-3 Distance relay model zone reach and delay settings

Protection zone	Zone reach (secondary Ω)	Time delay (s)
Zone 1	0.9943	0
Zone 2	1.732	0.5
Zone 3	7.912	1

Table A-4 National Grid network section data used for distance reach studies

Circuits	Length (km)	R_1(Ω/km)	R_0(Ω/km)	X_1(Ω/km)	X_0(Ω/km)	B_1(μS/km)	B_0(μS/km)
WBUR-HIGM	15	0.0275	0.1	0.2956	0.78	5.66	2.28
HIGM-RATS	65	0.0277	0.1	0.2971	0.78	4.38	2.28
WBUR-GREN	136	0.0271	0.1	0.2955	0.78	3.85	2.28
GREN-STAY	103	0.0278	0.1	0.2977	0.78	3.83	2.28
COTT-STAY	27	0.028	0.1	0.2975	0.78	3.83	2.28
STAY-RATS	43	0.0277	0.1	0.2975	0.78	3.83	2.28
RATS-WILE	22	0.026	0.1	0.2956	0.78	4.81	2.28

Appendix B Adaptive Distance Protection Simulink Model

This appendix briefly presents and describes the Simulink model and associated subsystems used to develop the adaptive distance protection scheme.

B.1 Complete subsystem

Figure B-1 shows the four subsystems constituting the full Simulink model. These represent the coordination layer and management layer functions of the adaptive protection architecture. An event generator subsystem is used to generate signals for testing the model. The reachability analysis subsystem contains the logic and Stateflow charts for conducting the safety verification presented in chapter 6.

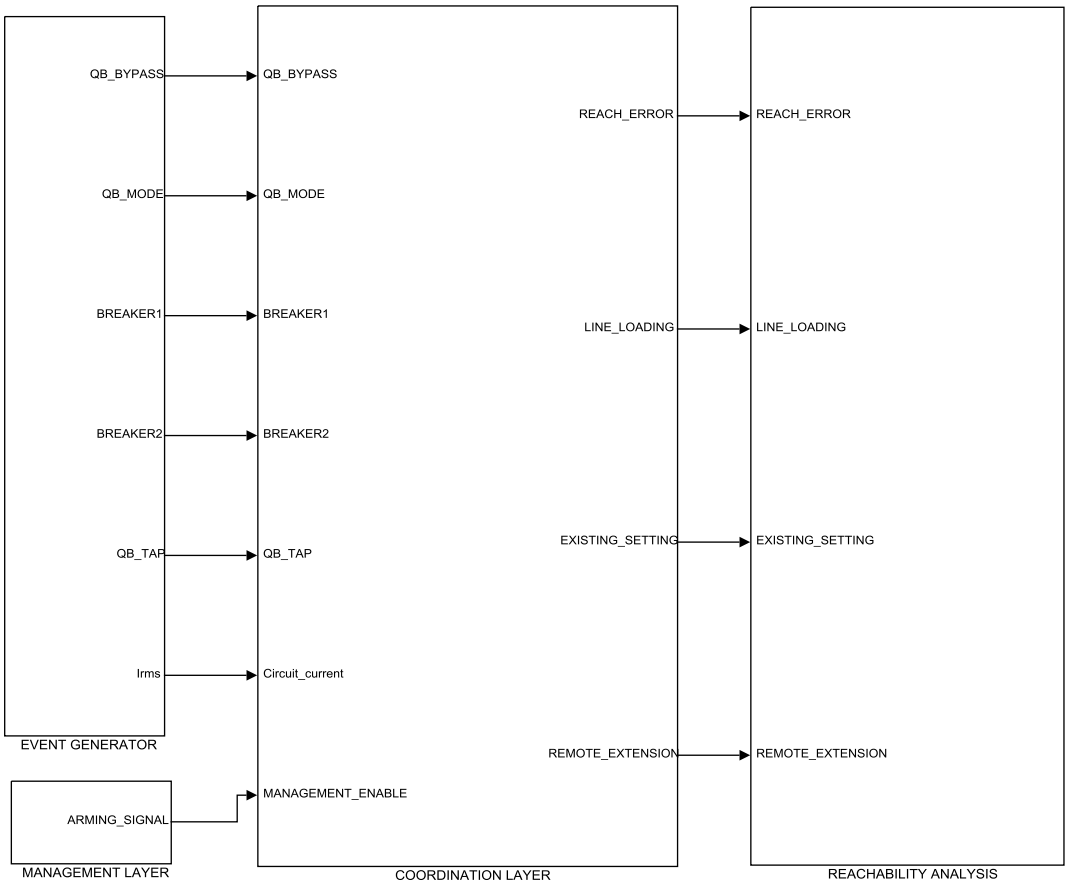

Figure B-1 Full high level Simulink model showing constituent subsystems

B.2 Event generator

The signal generator shown in Figure B-2 is used to generate events and signals for testing the complete Simulink model. Examples of the waveforms generated are shown in chapter 6 (Figure 6-15). Some of the signals are exported to the Matlab workspace for offline analysis. Furthermore, the signal 'Irms' is imported from the Matlab workspace to simulate transmission circuit loading to test the load encroachment scenario as explained in chapter 6 and Appendix C. The current signal is obtained from an RTDS simulation (as detailed in Appendix C) in a COMTRADE format and the raw data is imported to Matlab.

The signal generator block provides the ability to define pseudo random binary sequences that represent the QB states. This was used to stimulate the adaptive settings selection logic in the model as explained in chapter 6.

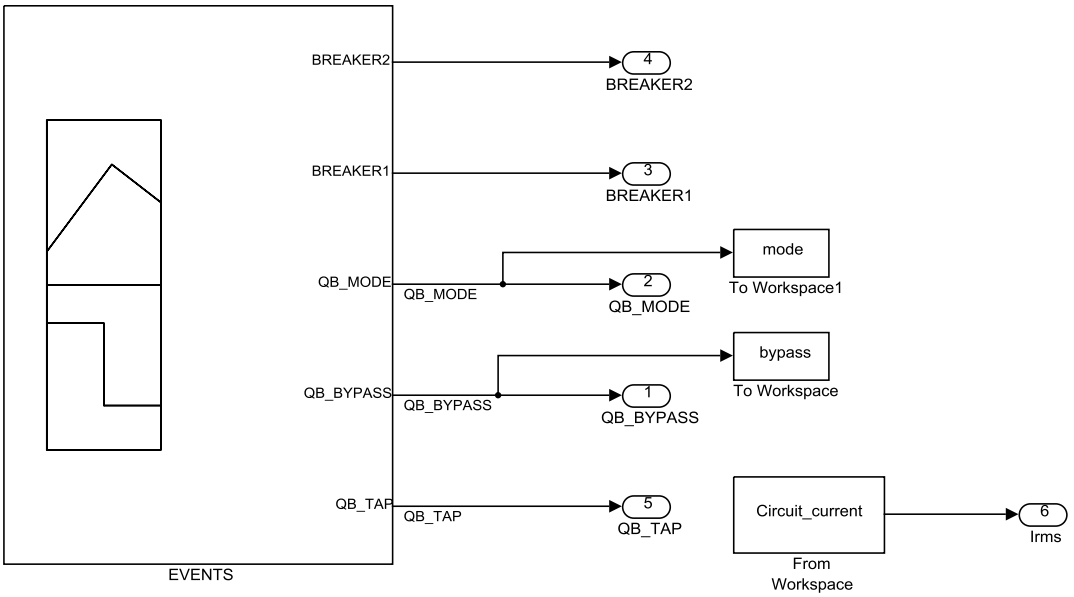

Figure B-2 Signal generator for testing the model

B.3 Coordination layer functions

Figure B-3 shows the overall coordination layer subsystem. This consists mainly of four functions that reflect the adaptive protection architecture definition. These are the ‘state acquisition’, ‘protection performance verification’, ‘protection setting select’ and the ‘setting apply and verify’ functions. In addition, a ‘reachability analysis signal mapping’ subsystem is created to propagate relevant signals to the reachability analysis subsystem. Some signals are monitored using a scope for troubleshooting.

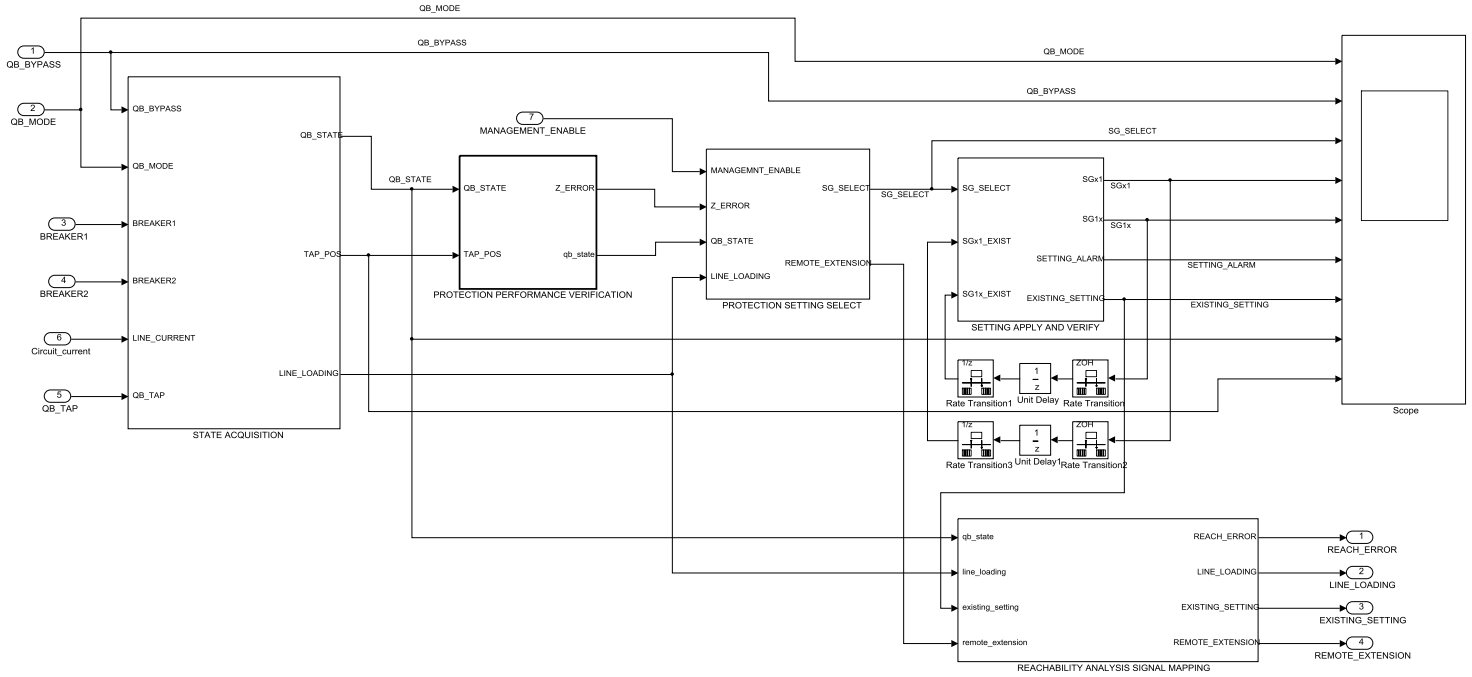

Figure B-3 Coordination layer subsystems

B.3.1 State acquisition subsystem

Stateflow charts have been used to determine the state of the QB and transmission circuit loading as shown in Figure B-4. Status measurements from the event generator subsystem are fed into the charts. When the model is deployed on the prototype target, the signals are obtained from the RTDS simulation. The tap position is propagated to the next subsystem (protection performance evaluation) directly.

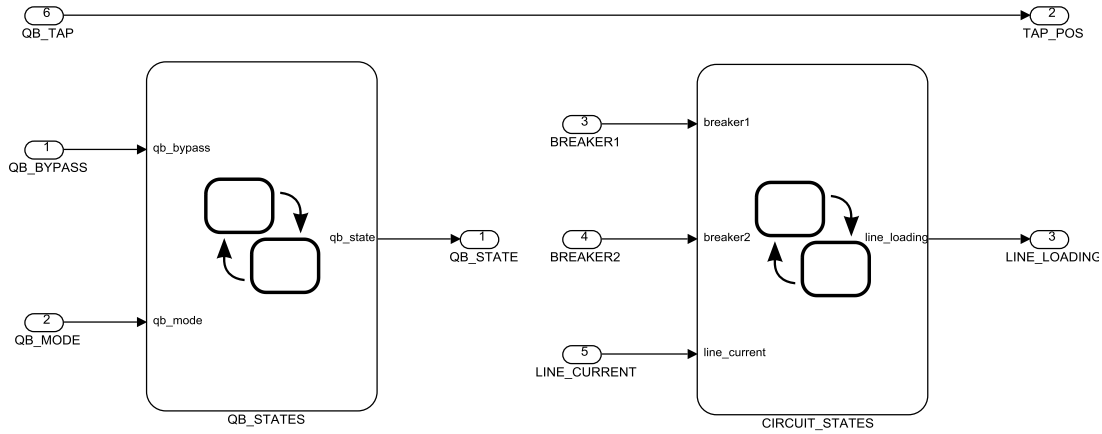

Figure B-4 Primary system state acquisition subsystems

The Stateflow chart 'QB_STATES' is shown in Figure B-5. The 'qb_mode' and 'qb_bypass' signals are used to determine the state of the QB (i.e. boost, buck or bypass). The QB states are enumerated throughout the model to simplify signal exchange and logic statements involving the QB state variables.

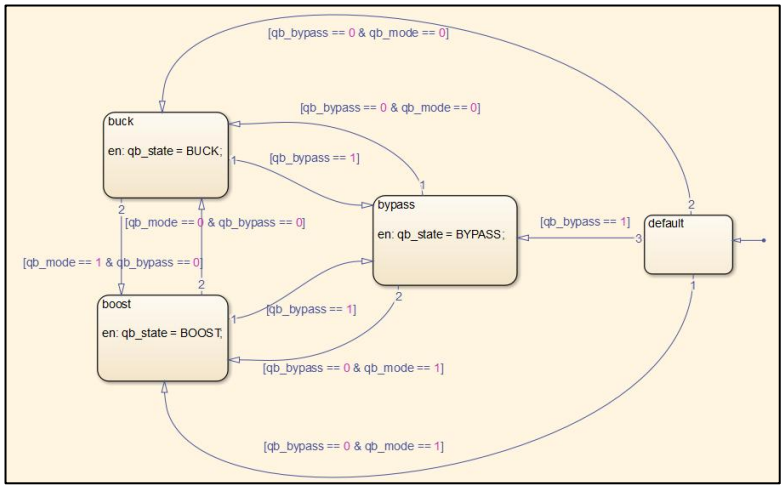

Figure B-5 Stateflow chart to determine QB state based on status measurements

Figure B-6 shows the Stateflow chart used to determine the state of the transmission circuit. Circuit breaker position status indications determine whether the line is energised or not. The level of line current flowing through the circuit determines whether the line is overloaded. Line overloading is defined based on the potential for load encroachment to occur as explained in Appendix C.

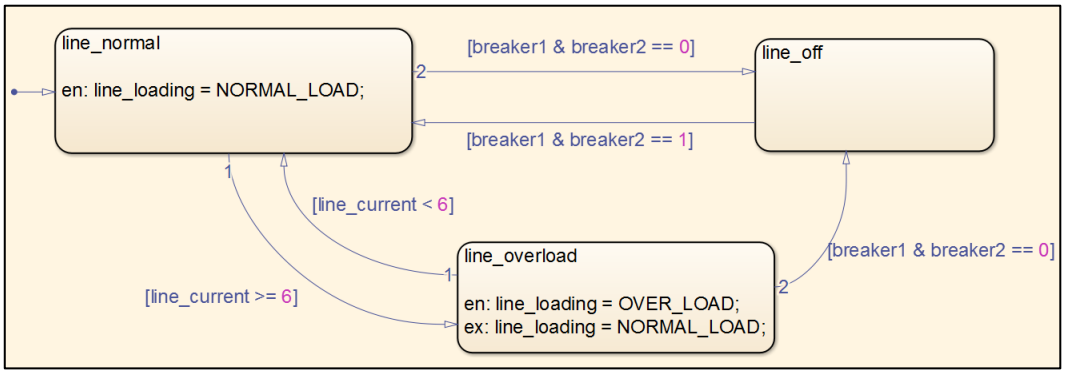

Figure B-6 Stateflow chart used to determine line loading state based on status measurements

B.3.2 Protection performance verification subsystem

This subsystem (Figure B-7) calculates the impedance error |ΔZ| based on the equation presented in chapter 3, section 3.4.5. The equation is implemented as Matlab code within the Matlab function block shown in the figure (the code is presented below). The associated variables presented in Table 3-8 are either hard coded in this subsystem or obtained through lookup tables.

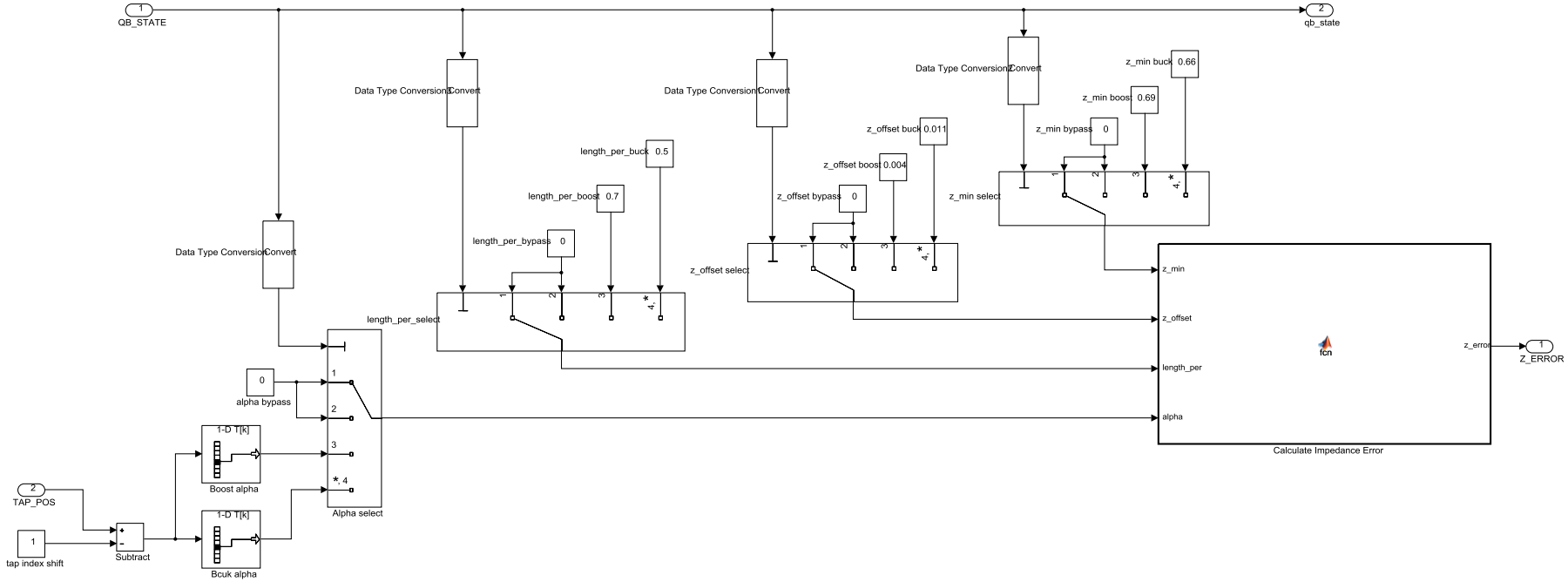

Figure B-7 Protection performance verification subsystem

```
function z_error = fcn(z_min, z_offset,length_per, alpha)
%#codegen

z_error = (z_min + (z_offset * length_per))*alpha;
```

B.3.3 Protection setting select subsystem

In this subsystem (Figure B-8), the impedance error calculated in the previous subsystem is compared with a predetermined threshold δ as discussed in chapters 4 and 5. If it is exceeded, then a change in settings is initiated.

The 'block_change' Matlab function block prevents the extension of the adaptive protection zone if there is a risk of load encroachment. Furthermore, the 'remote_coordination' Matlab function block sends a signal to a remote distance relay to extend its zone 2 reach if the remote line is short. Note that the remote zone extension functionality is not implemented in the prototype and is only a placeholder for future improvements. The associated code for the Matlab functions is shown below.

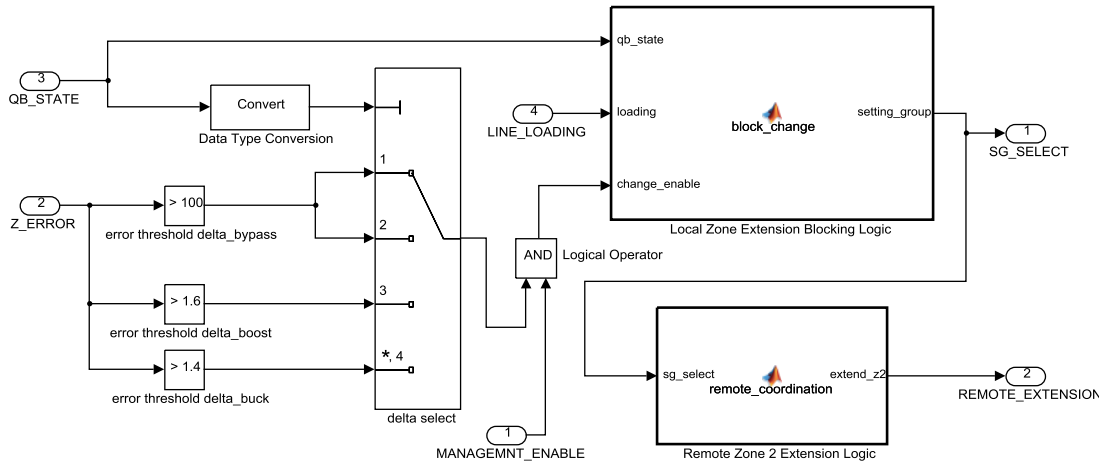

Figure B-8 Protection settings selection subsystem

```
function setting_group = block_change(qb_state, loading,
change_enable)
%#codegen

if(change_enable == 1)
    if (loading == 1)
       setting_group = 1;
    else
       setting_group = double(qb_state);
    end
else
    setting_group = 1;
end
```

```
function extend_z2 = remote_coordination(sg_select)
%#codegen

if (sg_select ~= 1)
    extend_z2 = 1;
else
    extend_z2 = 0;
end
```

B.3.4 Setting apply and verify subsystem

This subsystem (Figure B-9) implements the low level setting changes by manipulating the appropriate bits to be communicated to the protection relay. Further details can be found in chapter 5, section 5.5.4.

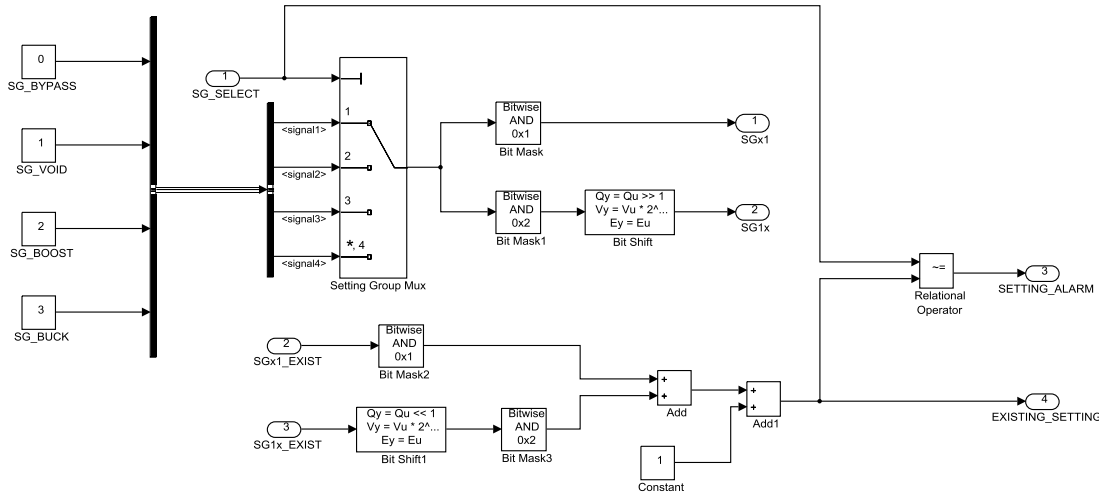

Figure B-9 Setting activation and verification subsystem

B.3.5 Reachability analysis signal mapping subsystem

The subsystem shown in Figure B-10 propagates the 'line_loading', 'existing_setting' and 'remote_extension' signals to the reachability analysis subsystem. Moreover, based on the 'qb_state' and 'existing_setting' signals, a new signal is generated ('reach_error') for use by the reachability subsystem. This new signal gives a numerical indication on whether the distance zone reach (defined by the existing setting) is under reaching, over reaching or neither. The stateflow chart (Figure B-11) and Matlab code used to generate this signal are shown below.

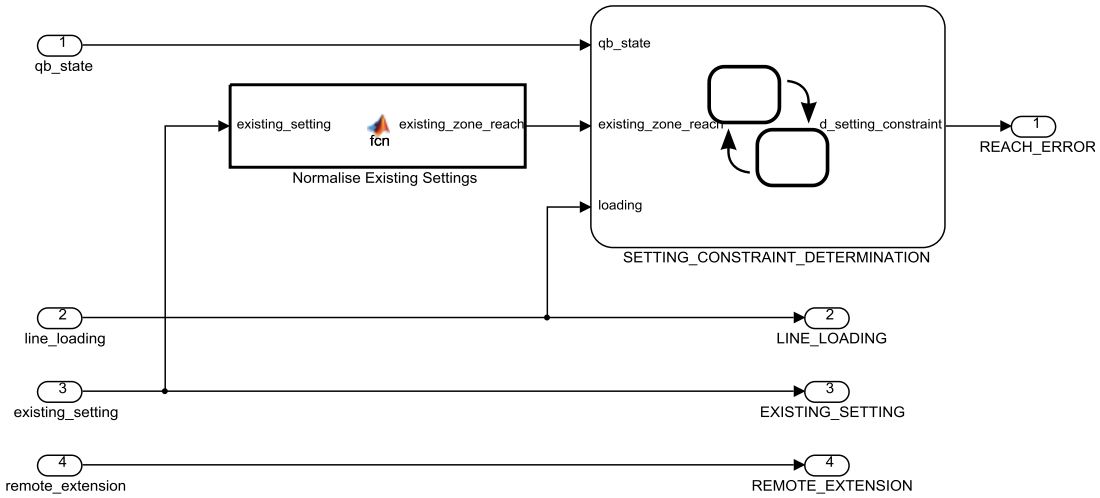

Figure B-10 Reachability analysis signal mapping subsystem

```
function existing_zone_reach = fcn(existing_setting)
%#codegen

switch(existing_setting)
    case 1
        existing_zone_reach = 1;
    case 3
        existing_zone_reach = 1.1;
    case 4
        existing_zone_reach = 1.3;
    otherwise
        existing_zone_reach = 1;
end
```

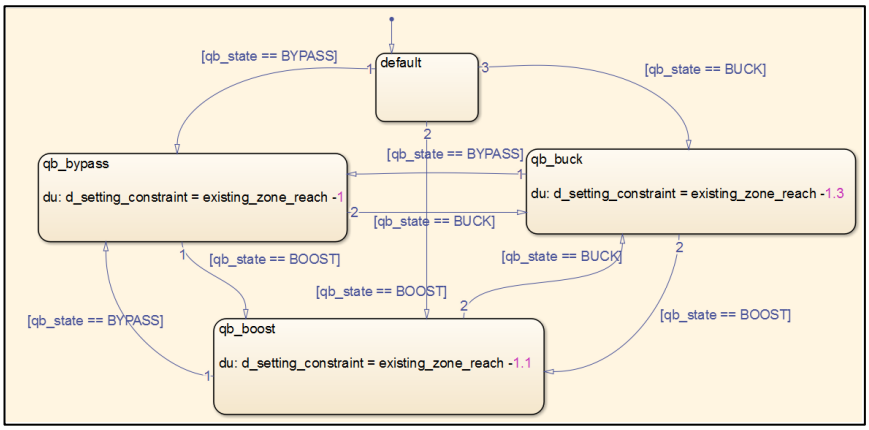

Figure B-11 Staeflow chart mapping QB state and protection setting for reachability analysis

B.4 Management layer functions

As mentioned in chapter 5, the implemented management layer functions are restricted to an 'enable' logic. The value of the logic must be set to '1' in order for the coordination layer functions to select a settings group other than the default one. This logic is propagated to the coordination layer as shown in Figure B-12.

Figure B-12 Management layer functionality

B.5 Reachability analysis subsystem

Figure B-13 shows the reachability analysis sub system. This has already been discussed in detail in chapter 6, section 6.5.1.

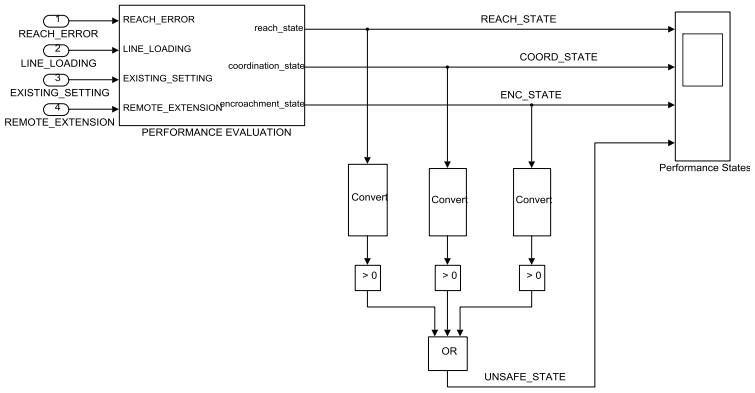

Figure B-13 Reachability analysis subsystem

Appendix C Load encroachment test scenario

Load encroachment was discussed in the thesis as a potential risk when adaptively extending zone 3. Moreover, the performance of the developed distance protection scheme during a potential load encroachment scenario was verified using reachability analysis. The network model and associated data to achieve load encroachment are included in this appendix.

Load encroachment is usually associated with networks long lines. So it was difficult to create such a scenario with the network used for testing in chapter 3. Therefore, the network shown in Figure C-14 was used to record the current threshold post load encroachment used in the reachability analysis. The data for the network model is shown Table C-5.

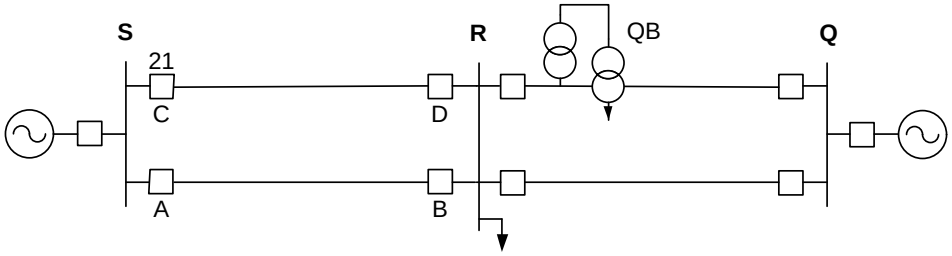

Figure C-14 Transmission circuit used for load encroachment

Table C-5 Transmission network model data

Line Impedances	Line Configuration	CT, VT Ratios
Z1 = 0.027+j0.296 Ω/km	Four single circuit segments	CT ratio = 1000:1A
Z0 = 0.1+j0.439 Ω/km	Segment length = 200km	VT ratio = 400kV/110V

A load encroachment scenario is created by increasing the protected circuit (C-D) through QB boosting action. This is then followed by the disconnection of the parallel circuit (A-B) which forces more power through the protected circuit. The impedance seen by the relay before and after load encroachment is illustrated in Figure C-15.

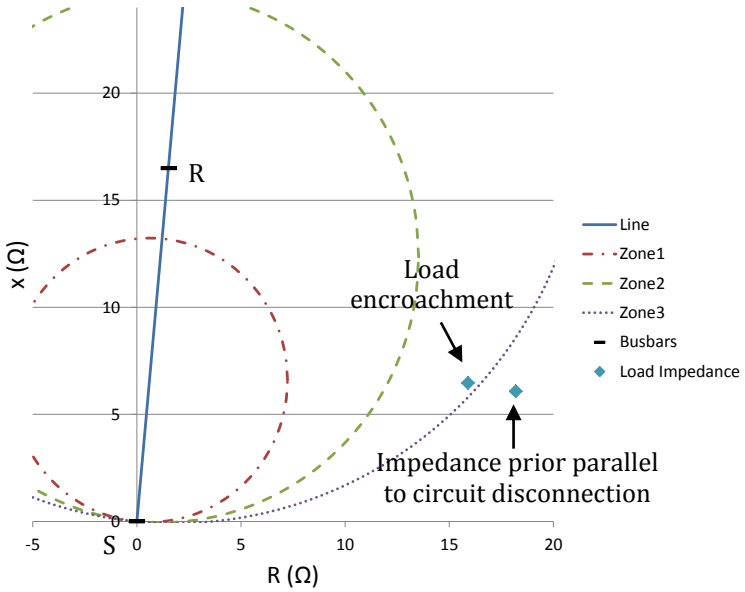

Figure C-15 Mho characteristic showing impedance pre and post load encroachment