Design of an Intelligent System for Validation of Protection Settings

Qiteng Hong

A thesis submitted for the degree of Doctor of Philosophy to

the Department of Electronic and Electrical Engineering

University of Strathclyde

June 2015

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.

Abstract

The reliable operation of protection systems depends on the correct settings of protective devices, which can be extremely numerous and complex within modern protection schemes. It has been realised that, despite multiple instances of checking, and verification and quality control processes, setting errors may remain undetected until an in-service mal-operation event is experienced. Furthermore, while the network evolves, the originally correct settings may be rendered erroneous under certain specific (unanticipated) situations. These issues present a strong need for a solution that allows comprehensive validation of settings and checking of the actual performance of the protection system with the settings applied in a variety of operational contexts.

To address these requirements, this thesis presents the outcomes of research concerned with developing and demonstrating an intelligent system-based solution incorporating hybrid Rule-Based (RB) and Model-Based (MB) approaches - the system has been termed the Power system Protection Smart Tool (PPST). It is shown that the combined RB and MB approaches are effective in complementing each other for the settings and performance validation tasks with enhanced reliability and automation. The advantages of the proposed methodology are demonstrated through case studies with actual network and settings data.

To maximise the applicability of the developed scheme, the considerable challenges of automating the use of existing settings data stored in a wide range of proprietary formats is also reported. A solution that has been developed which represents settings using IEC 61850 standardised file format and data model is described, along with a proposed methodology that will enable power utilities to migrate from existing approaches to the proposed future approach based on standardised protection settings. Adoption of these recommendations would facilitate a shift from protection systems being largely single-vendor solutions to becoming truly open platforms, capable of supporting the settings validation system as reported in this thesis and any other future applications that require access to

and/or manipulation of protection settings. Conclusions and future work concerned with moving the developed system to becoming a "business as usual" application are also included.

Acknowledgements

I'd like to thank my supervisors, Dr Adam Dyśko and Dr Campbell Booth, who have been extremely supportive to my research. Their guidance and inspiration are truly invaluable for my PhD and future career. I'd also like to express my gratitude to my colleagues in the Advanced Electrical Systems group at Strathclyde, who have been really kind and helpful.

Special thanks to Dr Victoria Catterson and Dr Steven Blair. I'm really grateful for their help and input to my PhD.

My gratitude extends to National Grid for the financial and technical support to this research. I'd like to thank Wen An (who is now working in China Southern Power), Tahasin Rahman, Nick Tart, Alasdair Chamberlain and Indy Sokhey for their valuable contributions to my work.

My sincere thanks also go to Dr Hon-wing Ngan and colleagues in Hong Kong Polytechnic University and CLP Power for hosting my visit to Hong Kong. The experience is extremely valuable to my research and future career.

Finally, I'd especially like to thank my families and friends for their support and encouragement over the years. This thesis is dedicated to them.

Contents

List of Figures

List of Tables

Glossary of Abbreviations

AC	Alternating Current
AI	Artificial Intelligence
ANN	Artificial Neural Network
API	Application Programming Interface
CB	Case-Based
CBR	Case-Based Reasoning
CX	Circuit Breaker
CIGRÉ	Conseil International des Grands Réseaux Électriques
CSV	Comma-Separated Value
CT	Current Transformer
DLL	Dynamic-Link Library
DNN	Deep Neural Network
EI	Extremely Inverse
EA	Evolutionary Algorithm
GB	Great Britain
GPS	Global Positioning System
GUI	Graphical User Interface
HV	High Voltage
HVDC	High Voltage Direct Current
ICD	IED Capability Description
IDE	Integrated Development Environment
IDMT	Inverse Definite Minimum Time
IEC	International Electrotechnical Commission

IED	Intelligent Electronic Device
JAR	Java ARchive
JRE	Java Runtime Environment
LHS	Left Hand Side
LV	Low Voltage
MB	Model-Based
MBR	Model-Based Reasoning
MV	Medium Voltage
NA	Not Applicable
OO	Object-Oriented
OP	Open Phase
Ph-E	Phase-Earth
Ph-Ph-Ph	Phase-Phase-Phase
PSCT	Protection Setting data Conversion Tool
PSRC	Power System Relaying Committee
PPST	Power system Protection Smart Tool
pu	Per-unit
Quad	Quadrilateral characteristic for distance protection
RB	Rule-Based
RCF	Residual Compensation Factor
RHS	Right Hand Side
SC	Short Circuit
SCD	System Configuration Description
SCL	System Configuration description Language
SCADA	Supervisory, Control and Data Acquisition
SGT	Super Grid Transformer
SI	Standard Inverse
SVC	Static Var Compensator
SWIG	Simplified Wrapper and Interface Generator
TXT	Text
TMS	Time Multiplier Setting

UML	Unified Modelling Language
VI	Very Inverse
VT	Voltage Transformer
WG	Working Group
XRIO	eXtended Relay Interface by OMICRON

Chapter 1

Introduction

1.1 Introduction to the Research

Protection systems defend power networks against abnormal operating conditions by isolating faulty components - typically within milliseconds - to minimise equipment damage, the risks of wide-area blackouts, and other unsafe or undesirable conditions. The reliable operation of protection systems depends on the correct design and application of numerous configuration parameters within protective devices, such as the status (enabled or disabled) of protection functions, distance protection zone reaches, overcurrent protection pick-up current, etc. These parameters are known as "protection settings".

There are numerous examples of evidence which indicated that relying solely on protection engineers for decision making and validation in the setting of protective devices can still lead to some unexpected (or hidden) errors, despite multiple instances of checking, and thorough verification and quality control processes [Sie11a, AS09, Uni04]. These errors may result from erroneous calculations, from engineers' misunderstanding or mistranslating of setting policies, or from potential errors in the process of the application of settings to the protection devices or in the approval or commissioning processes. Failure to identify these errors may result in in-service mal-operation events, or even large-area blackouts [Uni04, AS09].

Furthermore, power networks have been experiencing, and will continue to experience, significant changes over recent years, with the decommissioning of large-scale fossil-fuelled synchronous generation, the introduction of converter-interfaced sources and HVDC interconnectors both between separate systems and within large systems, potential incorporation of large-scale energy storage, the increase of system loading, varied fault levels, etc. [Wor07, Mac08] These changes mean that existing setting policies or knowledge may no longer be adequate or valid under all circumstances. The originally correct settings may be rendered erroneous under certain specific (unanticipated) situations. These issues result in a strong requirement for a method and associated tools that are capable of comprehensively assessing and validating existing protection settings.

Increasing network complexity and the large number of protective devices in the system mean that a manual process for validation of protection settings can be extremely challenging. In 2003, National Grid in the GB had to undertake an urgent review of 41,264 relays with approximately one million separate parameters in four weeks following a protection mal-operation event in London [Uni04, Nat03]. Although the task was completed in four weeks, it required urgent arrangements with significant manual input (e.g. a fully dedicated team, appointment of external contractors, etc.), which can be very costly. The surveyed relays are for backup protection and mostly with conventional types (e.g. electromechanical relays), each of which only contains multiple setting parameters. The task may be further challenged with the introduction of multi-function numeric protection Intelligent Electronic Devices (IEDs), where hundreds of setting parameters may be available in each device [SMB+10]. Validation of a single modern protection scheme with protection IEDs can take hours of an engineer's fully dedicated time. In practice, the time budgeted for such a task can be more than a week due to the availability of engineers. Given the numerous protection schemes available in the network, the validation process can be extremely time-consuming and costly if conducted manually. Furthermore, a manual validation process is also subject to additional human errors, which is not fully reliable.

Existing work in the area of protection settings has mainly focused on the

automation of the protection settings calculation and coordination functions [EAJMB05, LL96, LYYJ90, KSS97, KSK+93, SL00]. Such systems are not readily suitable for the settings validation task for the following reasons: a range of setting values can be valid, so any inconsistency between the calculated values and the actual settings cannot be used to indicate errors; the validation of settings also involves the checking of the functional configuration, which is difficult to be achieved by these calculation tools. There are existing systems can be used for the validation of settings [BGK+14, A. 14, ETA15, Ele15]. However, such systems provide no check against setting policies, which is not acceptable for a practical system. Furthermore, these systems are mostly Model-Based (MB) and require significant manual input for the population of network models, configuring protection IED models, analysing simulation results, etc.

The research reported in this thesis is concerned with the design of a method and an associated intelligent system that allows comprehensive and automatic validation of protection settings. The suitability of existing Artificial Intelligence (AI) techniques for validation of protection settings is investigated and assessed in the context of practical industrial applications, and based on this analysis, a hybrid Rule-Based (RB) and MB approach has been proposed and implemented. Such an approach is considered to be the most suitable solution for addressing the settings validation and protection performance verification challenges.

The RB module checks the settings against network operators' setting policies and experts' knowledge, ensuring that all the settings are compliant with the associated regulations. The MB module performs further means of checking through simulation-based validation of the actual performance of the protection system in the context of the element(s) of the primary system that are protected, using a fully integrated modelling environment that sources system data and drives the simulation package used by the network operator (in this research, the work was funded by National Grid and the system has been developed to integrate with their information systems but, as far as possible, the system has been developed to be generically applicable).

The entire validation process is automated. Specifically, significant manual

input, as is often required in existing MB systems, is avoided by a mechanism that allows the interaction with a commercially-available simulation engine to manipulate its function and data for the settings validation task. The simulated results returned from the MB module are automatically analysed by the RB module. The combined RB and MB approaches are proved to be effective and complementary, offering a satisfactory solution for the settings validation task. The highly automated validation process allows the time required for validating a modern protection scheme to be scaled down to minutes from days. In this thesis, the methodology is demonstrated through the design and implementation of an intelligent system PPST. The key advantages of such a system are demonstrated through case studies based on actual network and settings data in the GB transmission network.

One of the major challenges encountered in the design and implementation of PPST is the difficulties associated with manipulating existing settings data stored in proprietary file formats. This can introduce a significant burden in the development and maintenance of the system. Such difficulties are also experienced by any software applications that require access to and manipulation of protection settings data. The dissertation documents the investigation of said challenges and describes a proposal to address these problems through the use of the data model provided by IEC 61850 [IEC10a] with the System Configuration description Language (SCL) format to represent protection setting data in a standard fashion.

The benefits of such a standardised approach are evaluated and a solution that allows network operators to migrate from existing approaches to the new approach based on the use of standardised settings is explained and demonstrated.

1.2 Justification for Research

RB expert systems have been extensively used in power system applications, including power system event classification and analysis [SBG02], protection failure and event diagnosis [MDM+96, VRF+99, PWN92], and service restoration and planning and implementation of remedial actions [KV91, PL97]. The successful

application of RB systems has automated laborious tasks and provided extensive support for engineers in some cases. The function of validation of settings is mainly based on network operators' setting policies and experts' knowledge, which can largely be represented readily in the form of rules, making them naturally suited to implementation in an RB system [HDB12]. RB systems also provide excellent explanation facilities, which is extremely useful for locating the identified errors and making suggestions for corrections and remedial action.

However, the main shortcoming of RB systems in the context of this work is that when specific problem instances or scenarios are not defined in setting policies and therefore excluded from the rule base, the system may fail in detecting specific errors. Furthermore, the RB approach is not capable of assessing the validity of the actual setting policies themselves.

These problems can be addressed by MB systems, which contain functional knowledge of the physical systems and are capable of simulating a wide range of system conditions and the correct (and certain modes of incorrect) protection responses, including those that may not be anticipated during configuration and setting of the protection systems.

However, MB systems may encounter difficulties in fully encompassing the setting policies within the performance validation process. For example, it is required that differential settings should be the same at all ends of circuits and the functions within the multi-functional IEDs should be configured (enabled or disabled) as required. Such checks can be difficult to be achieved solely by the MB approach since the settings violating the policies may still function correctly in response to certain fault events. As discussed previously, the checking against setting policies is more suitable to be addressed using an RB approach, hence the complementarity of the two approaches. The RB approach can also facilitate the automation of the MB validation process, e.g. analysis of the simulation results, thus minimising manual input.

Existing setting files stored in various formats have introduced significant challenges for developing and maintaining systems that require access and manipulation of protection settings [A. 13b, AV07, CBB+13, HBC+13, SMB+10],

including the settings validation system as reported in this thesis. Furthermore, the existing approach for representing and managing protection settings is considered complex, resulting in inefficient system engineering and management [SMB+10, Apo05, E3 10, Bur12, G. 14, X. 14a, ENT12]. These challenges are investigated in the research reported in this dissertation, and a solution to represent settings data in a standardised format and data model provided by IEC 61850 is proposed. The key benefits of such an approach is that it eliminates the need for proprietary file formats and software tools, and allows a more efficient engineering process to be developed. The standardised format of protection settings is easier to interpret and manipulate using software, which significantly reduces the burden of designing, implementing, and maintaining protection schemes. The proposed approach offers support to the PPST and any other systems that require access and manipulation of protection settings.

Through the presented work, the thesis considers all aspects associated with the automatic validation of protection settings task, from the data manipulation to the reliability and automation of the intelligent system. Adoption of the methodologies and recommendations allows comprehensive validation of settings to be performed with minimal manual input required and facilitates a more efficient process for protection systems management and engineering.

1.3 Principal Contributions

This research provides the following contributions to knowledge:

- Comprehensive investigation of AI techniques that are suitable for validation of protection settings and proposal of a novel methodology that applies a hybrid RB and MB approach for settings validation, which is capable of effectively performing the targeted task with enhanced system reliability and automation.

- Implementation of a hybrid intelligent system (PPST) that combines RB and MB modules for the validation of protection settings and demonstration of its operation in two case studies.

- Design and demonstration of the operation of an RB module that performs the tasks of automatic protection settings validation and MB results analysis within a hybrid system, and development of associate rules for performing such tasks.

- Design and demonstration of the operation of an MB module that allows MB settings validation through the interaction with a commercially-available simulation engine, where an automatic process is established to populate equivalent network models, install and configure relay models, create and simulate system events, and analyse simulation results to highlight identified abnormal protection operations.

- Investigation of challenges in manipulating existing proprietary protection settings data and a proposal and demonstration of the use of standardised data model and file format provided by IEC 61850 to represent settings. The proposed approach simplifies the manipulation of settings data for future automatic applications and settings data management.

- Proposal of a novel IED configuration process based on the common representation of protection settings, which is significantly streamlined compared with existing processes and simplifies the task for the design and implementation of multi-vendor protection, automation and control systems.

- Design and implementation of a tool that allows automatic bi-directional translation between proprietary settings and IEC 61850-based settings. A methodology for code generation element is proposed and implemented to facilitate the rapid development of functions to support the settings data conversion between proprietary formats and the standardised format for new relay types and protection functions. This provides a solution for utilities to migrate from existing proprietary approaches to the future approach based on the standardised settings.

1.4 Thesis Overview

This thesis is organised as follows. Chapter 2 provides an overview of power system protection, including its role in power system operation, the main protection functions and their fundamental principles, and the various tasks and considerations associated with protection settings. Existing activities and tools that are associated with protection settings are reviewed and discussed.

Chapter 3 reviews a number of AI techniques and their applications in power system protection, based on which a hybrid RB and MB approach is proposed for the protection settings validation task. The reasons of why such an approach is selected are discussed.

Chapter 4 presents the process and outcome of the investigation of the challenges in manipulating protection settings data stored in proprietary formats. A standardised approach is proposed for representing the settings data. The key benefits of such an approach are discussed. The methodology for network operators to migrate to the proposed approach from existing approaches is also presented.

Chapter 5 presents the details on the proposed hybrid RB and MB methodology through description of the design and operation of the intelligent system PPST.

Chapter 6 presents two case studies using actual network data and setting files to demonstrate how the RB and MB modules can be used for identifying setting errors, and how the proposed hybrid system can offer an improved system performance with enhanced reliability and automation.

Chapter 7 summaries the work presented in the thesis, highlights the key challenges faced and the contributions of the research to address these challenges. Suggestions on the further investigation and research are also provided.

1.5 Publications

The following publications have been completed during the course of this PhD:

1.5.1 Journal Article

Enabling Efficient Engineering Processes and Automated Analysis for Power Protection Systems
Q. Hong, S. Blair, C. Booth, V. Catterson, A. Dyśko, and T. Rahman,
submitted to *IEEE Journal of Systems*

1.5.2 Conference Papers

A Model-based Approach for Automatic Validation of Protection Settings
Q. Hong, C. Booth, V. Catterson, and A. Dyśko
PAC World Conference, Glasgow, UK, 2015

Improving IEC 61850 interoperability and simplifying IED configuration through the standardisation of protection settings
Q. Hong, V. Catterson, S. Blair, C. Booth, A. Dyśko, and T. Rahman
CIGRÉ Session, Paris, France, 2014

Translating Proprietary Protection Setting Data into Standardised IEC 61850 Format for Protection Setting Validation
Q. Hong, A. Dyśko, V. Catterson, C. Booth, S. Blair, and T. Rahman
IET Developments in Power System Protection (DPSP), Copenhagen, Denmark, 2014

Standardisation of Power System Protection Settings Using IEC 61850 for Improved Interoperability
Q. Hong, S. Blair, V. Catterson, C. Booth, A. Dyśko, and T. Rahman
IEEE Power & Energy Society General Meeting, Vancouver, Canada, 2013

Intelligent System for Detecting "Hidden" Errors in Protection Settings

Q. Hong, A. Dyśko, and C. Booth

International Universities Power Engineering Conference (UPEC), London, UK, 2012

Chapter 2

Review of Fundamentals of Power System Protection

2.1 Introduction

This chapter reviews the fundamentals of power system protection. Focus is placed upon the topics associated with protection settings, which is the main application area covered by this research. It starts with an introduction of electrical faults, which are the main abnormal conditions that protection systems operate against and the key elements to consider during the setting of protection devices. Section 2.3 provides an overview of protection systems, which covers the operating principles, main protective devices, issues associated with reliability, and the role of protection settings. In Section 2.4, the main protection functions used in transmission networks are introduced, along with discussions of the main considerations in setting the said functions. The management of protection settings over their life cycle is introduced in Section 2.5, which is an important consideration such that a solution of settings validation can be developed to best fit within the processes adopted within any particular organisation and to maximise the potential usage of the developed system. In Section 2.6, a review of existing activities associated with protection settings is presented, and the reasons why existing systems are not readily suited the settings validation task are discussed.

2.2 Electrical Faults

Electricity is transmitted from generation sources to end users through power networks and faults may occur at any point on the networks. As shown in Figure 2.1, the generated electrical energy is firstly stepped up to high voltage levels (typically 400 kV, 275 kV and 132 kV in the GB) to minimise current and therefore losses for large power transfers. The electricity is then transmitted over long distances through transmission networks and stepped down to appropriate voltage levels (typically 33 kV, 11 kV and 240 V) to supply consumers through distribution networks.

Electrical faults are phenomena that lead to abnormal currents and voltages in the power networks, which can mainly be categorised as open phase (OP) and short circuit (SC) faults [IEE06]. OP faults are typically caused by broken conductors. [SKS+00, RBM01] report a number of research activities concerned with the detection of OP faults. In the context of power system protection and as the main topic of this thesis, the vast majority of electrical faults are SC faults in nature, which are characterised by the presence of high currents in the network - the current only being limited by the impedance from the sources to the fault (and the return path) and the short circuit current provision capability of the sources supplying the current to the fault. SC faults, if not isolated in a timely fashion and in the proper fashion (i.e. ideally only isolating the faulted component or network section), may cause severe damage to electrical equipment, system-wide disturbances, or even wide-area blackouts.

In three-phase AC power networks, SC faults mainly have the following types (as illustrated in Figure 2.2): phase-to-earth (Ph-E) fault, phase-to-phase (Ph-Ph) fault, two-phase-to-earth (Ph-Ph-E) fault, and three-phase (Ph-Ph-Ph) fault [Y. 13]. Z_f is the fault impedance, and the faults with zero impedance are called bolted SC faults [GSO12]. SC faults can also be classified as symmetrical and unsymmetrical types. Symmetrical faults are three-phase balanced (e.g. Ph-Ph-Ph faults), whereas unsymmetrical faults are unbalanced in three phases (e.g. all fault types except Ph-Ph-Ph faults as shown in Figure 2.2).

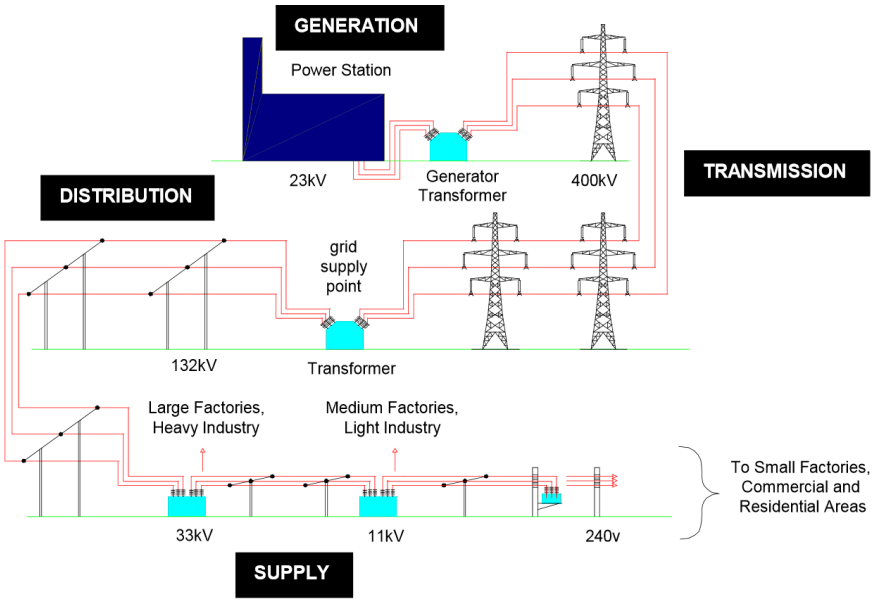


Figure 2.1: A typical power network [But01]

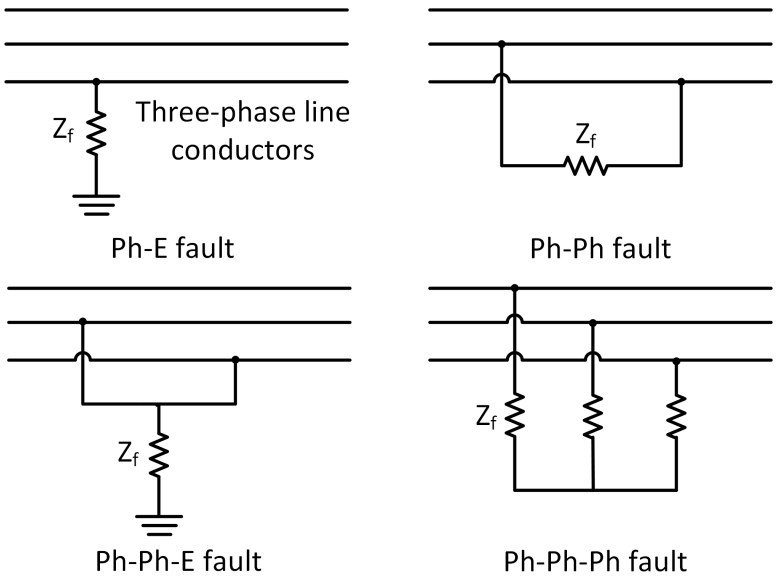


Figure 2.2: Main SC fault types in three-phase AC networks [Y. 13]

Power system element	**Probability of faults(%)**
Overhead lines	50
Underground cables	9
Transformers	10
Generators	7
Switchgear	12
Other equipment	12
Total	100

Table 2.1: Proportion of all faults experienced by various power system elements [Y. 13]

SC faults are mainly caused by the failure of insulation, which can be as a result of overvoltage (e.g. induced by a lightning strike) or the weakening of the insulators caused by ageing, chemical pollution, snow, etc. [Y. 13] Table 2.1 lists the statistics of proportion of all faults experienced by various power system elements. It can be seen that the overhead lines have by far the highest risk of faults. Therefore, it is prudent to use overhead line protection as examples and case studies for illustration of the proposed methodology for protection settings validation in this thesis, although the method is applicable to any and all protection settings functions and applications.

Fault level calculations and flows of fault currents through the various paths are key for determining protection settings. National Grid (and other transmission network operators) typically carries out comprehensive fault studies on an annual basis and publishes openly the associated results - both for the present system configuration and for a period of several years into the future using information relating to anticipated future changes to the system [Nat14]. The calculated fault current can, for example, be used in the selection of pick-up current setting and time dial value of the overcurrent protection scheme so as to provide fast operation and proper coordination with other protective equipment (more details on this topic are presented in Section 2.4). The methodology for calculating currents for various fault situations can be found in [IEC01].

2.3 The Protection System

2.3.1 Overview

The protection system defends the power network against the most potentially severe consequences of faulty conditions by detecting and isolating faults within milliseconds so as to minimise the damage to equipment and disturbances to the overall system. Figure 2.3 shows the main elements in a typical protection system. The voltage transformer (VT) and current transformer (CT) are measurement devices that sense the voltage and current in the primary system, convert the quantities to appropriate smaller-scale secondary values, and feed them to the protection relays, which are the main protective elements that contain logic and algorithms to determine the existence of faulty conditions that they may be required to react to (more details on protection relays are available in Section 2.3.2). Sometimes only VTs or CTs are used, depending on the type of protection. If a fault is detected, the relay, if responsible for the main protection function of the item of equipment upon which a fault has been detected, will issue a tripping signal to associated circuit breakers (CXs) as quickly as possible, which will then operate to isolate the faults from the system. If the protection detects the fault but determines that the fault is remote, then it may delay its tripping output so that other protection systems closer to the fault location may react first - if the fault is detected as still being present on the system after a pre-determined time delay, then the relay may trip to provide backup.

In some cases, e.g. differential protection, local measurement information is not adequate for detecting faulty conditions, so communication links are required to obtain required measurements from other sources (e.g. the remote end relay for the protection of a transmission line)[Bla13]. Communications may also be used to transfer tripping (or inhibiting of tripping) signals between protective devices. It is clear that the operation and configuration of protection schemes can be a complex task.

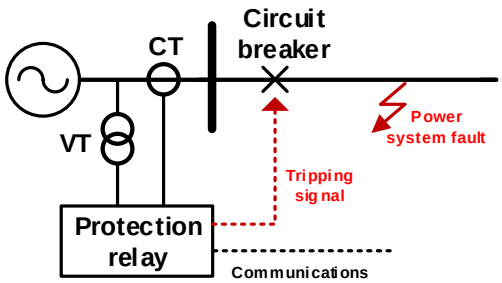


Figure 2.3: Main elements in a typical protection system

2.3.2 Protective Relays

As already stated, the protective relays are key elements within a protection system, and are responsible for detecting faults and making decisions on actions to take when a fault occurs such that only a minimal element of the faulted power system is disconnected. As shown in Figure 2.4, the development of relay technology can be classified into four main stages, from the earliest electromechanical devices to modern state-of-the-art numerical relays, often employing multiple microprocessors within a single unit.

In this thesis, focus of investigation and development is on the validation of settings and the anticipated in-service performance from numerical relays, although all relay types may still be employed in existing systems. This is because: numerical relays are being increasingly used and any new devices installed in the transmission system are invariably of numerical type; numerical relays normally have many more settings than the other relay types, so they represent the main challenges for settings validation. The methodology presented in this thesis is equally applicable to all relay types. The only difference is the way of accessing and manipulating the protection settings data, since numerical relays are normally equipped with software tools for management of settings, while other types of relay do not have such features. The following paragraph provides an overview of numerical relays, and the details of other types of relay can be found in [Gri11].

Numerical relays were firstly introduced in around 1985. They are also referred as protection IEDs. These types of relay are equipped with advanced computing technologies, which allows efficient real time signal processing and algorithm

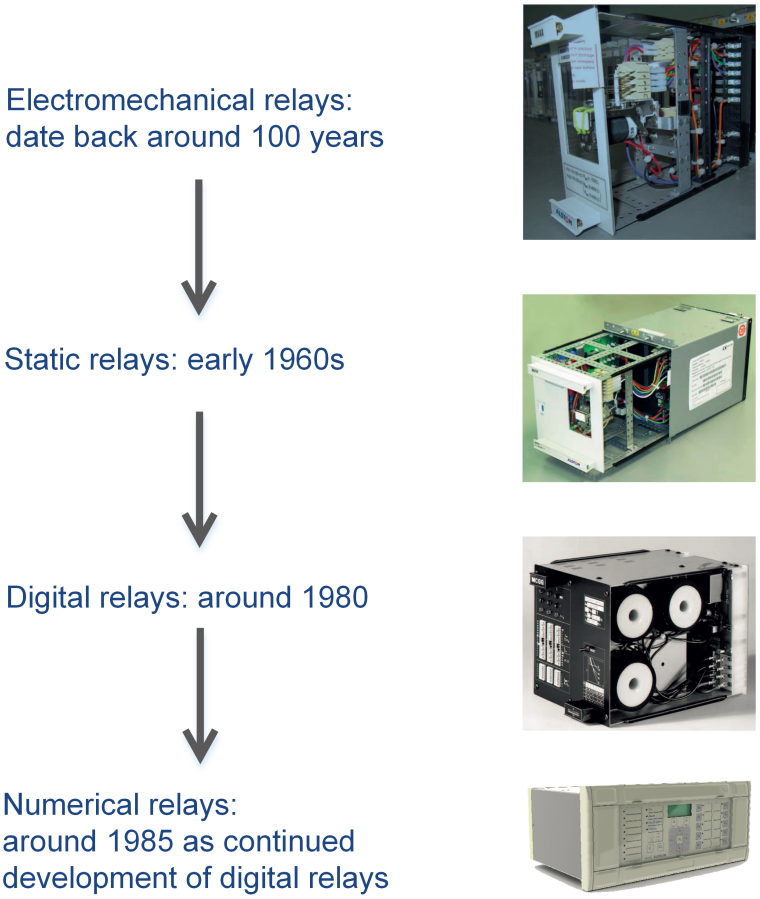


Figure 2.4: The development of relay technology [Gri11]

executing. Powerful microprocessors with relatively large memory capacities are used, allowing multiple protection functions that were implemented previously using separate devices to be integrated into a single element. While the capability of numerical relays has been significantly enhanced compared to other relays, there are concerns from engineers and users over the potential degradation of reliability as a result of integrating multiple protection functions in one device [Gri11]. To allay those concerns and improve performance, many numerical relays are equipped with self-monitoring functions. In practice, while a single numerical relay may be capable of providing multiple protection functions, each protection scheme is equipped with dedicated devices to avoid failure of multiple protection functions resulting from a problem with a single multi-functional device. This is particularly evident in transmission networks protection, where high reliability of the protection system is required.

2.3.3 Reliability of the Protection System

The reliability of protection systems can be measured by its dependability and security. The dependability is the degree of certainty that a protection system will operate when it is required, while the security is the degree of certainty that a protection system will not operate when it is not required [SMB+10]. Dependability requires the protection system to be sensitive enough to detect faulty conditions, i.e. faults within the protected zones. Security requires the protection system to remain stable (i.e. not to operate) for non-fault conditions, transients and for external faults to which the protection system in question should not respond. Furthermore, protection may be required to respond instantaneously to certain faults, but with a delayed operation if operating in backup mode. Therefore, a protection system responding either more quickly or more slowly than required could be classed as an error and a degradation.

To enhance the reliability of protection systems, duplicate, and in some cases triplicate, levels of redundancy are employed in the main protection schemes by transmission network operators in GB, with one or two dedicated backup schemes also being applied. The reliability is subject to a wide range of factors, which can

be summarised as follows [SMB+10]:

- Design of protection schemes. A proper design will make sure the protection system still provides adequate functionality to isolate any abnormal conditions even with the loss or malfunction of certain components. This is normally achieved by careful selection of protection functions and manufacturers' devices to be used, duplicating main protection functions, and the properly use of backup protection both locally and from adjacent circuits. Protective devices from different manufacturers are commonly used within a single scheme to provide redundancy so as to ensure that any common or design-mode failures introduced by a specific manufacturer do not result in the complete failure of the scheme, as might be the case with duplicate devices from the same manufacturer.

- Setting of protective devices, which includes the correct configuration of functions, correct calculation of numerical settings, etc. Proper settings allow only faults within protected zones to be isolated while maintaining the stability against non-fault conditions and external faults.

- Maintenance of protection system. Regular maintenance of the protection assets (including review of settings) is essential to ensure the system is compliant with all requirements specified in associated standards or guidance documents.

- Failure of physical devices such as relays, CXs, communication channels, etc. This is normally addressed by careful modelling of these devices and applying probabilistic analysis of potential failures, thus to analyse and quantify potential risks so that mitigating actions may be taken if required.

Apart from the last factor that is relevant to hardware devices, the other three factors can be relevant (to an extent) to the protection settings validation task. For protection schemes, it is important to make sure that the protection functions being used conform to the design and policy and that the correct protection devices (relay type, production model, etc.) have been used. The settings of

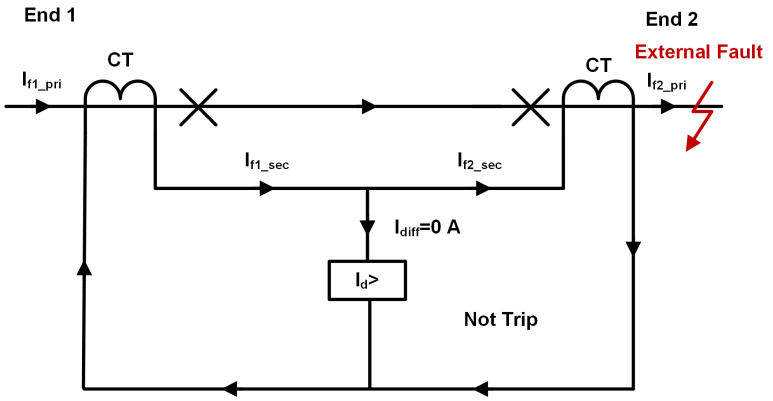
protective devices can be validated before implementation to minimise the risk of errors. The maintenance of the system, which includes the review of settings data is essentially a repeat of the settings validation task. Therefore, a solution that allows comprehensive protection settings validation, if correctly designed and implemented, will act to enhance the reliability, and potentially improve the performance of the protection system. The factors described above are taken into account during the investigation of such a solution as reported in Chapter 5.

2.4 Main Protection Functions

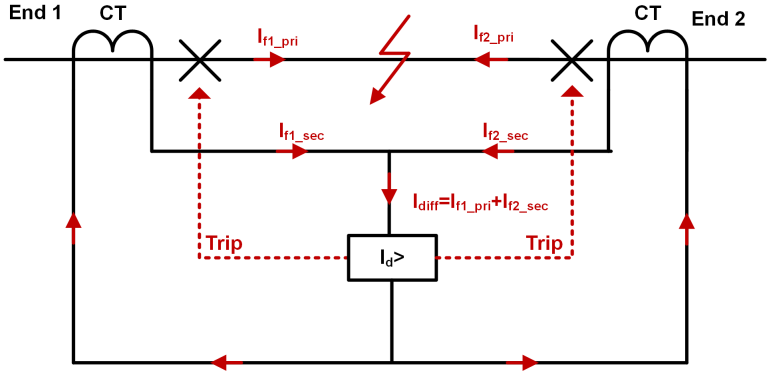
In this section, a brief review of main protection functions used in transmission networks is provided, which includes differential, distance and overcurrent protection. The main considerations for setting these functions with regards to overhead line protection are discussed. Other protection functions that are frequently used in power systems include over/under-voltage protection, over/under-frequency protection, circuit breaker fail protection, transformer and busbar protection, etc. To enhance brevity and relevance of this section, these are not included in this chapter and more details on these protection functions can be found in [Gri11].

2.4.1 Differential Protection

Differential protection is a form of unit protection, which only detects and isolates faults within a certain zone without reference to other parts of the network. In the GB transmission network, it is mainly used for the protection of feeders, transformers and busbars. The operating mechanism of differential protection is based on the Merz-Price principle [Gri11], which is illustrated in Figure 2.5. For an external fault (Figure 2.5a), the current at End 1 and End 2 have same magnitude and direction, so the secondary current I_{f1_sec} and I_{f2_sec} equals to each other both in magnitude and direction, resulting in zero differential current (i.e. I_{diff} =0 A) so the protection stays stable, although in practice there may be errors in CT outputs during external faults due to inaccuracies or saturation



(a) External fault



(b) Internal fault

Figure 2.5: Basic principle of differential protection

at high current levels, but biasing and other means of addressing this have been successfully developed and incorporated within differential protection systems. More details on this are included later.

If an internal fault occurs as shown in Figure 2.5b, the current at the both ends will have different directions and it is highly probably that they will also have different magnitudes. As a result, the currents from each end will both contribute to I_{diff}, which is normally much larger than the relay current setting thereby triggering the protection operation.

Figure 2.6 shows a typical arrangement of practical overhead line differential protection using numerical relays, where communications between the local and remote end relays are used for the comparison of the measured current thus to determine the existence of fault conditions.

In reality, as mentioned previously, even for external faults or under normal

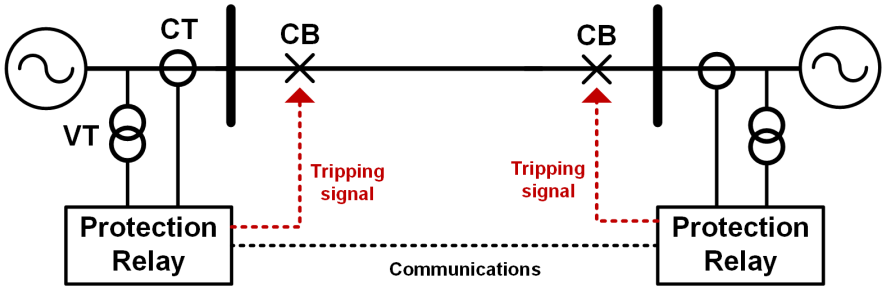


Figure 2.6: Two-ended differential protection using numerical relays [Bla13]

operating conditions (especially during heavy load conditions), currents measured at both end may not be identical. The difference between the these currents is called spill current, which is caused by a number of factors including: the CTs on both ends are not totally identical; the transmission line's shunt capacitance leads to line charging current, which would be taken from the inward current; and the circuits are not entirely symmetrical at the two sides.

To avoid mal-operation resulted from spill current, numerical IEDs normally adopt a biased operating characteristic as shown in Figure 2.7, where I_{s1} is the minimum pick-up current setting; I_{s2} is the biased current threshold beyond which a different biased slope is used; and k_1 and k_2 are the settings to control the slopes of the biased characteristic. For internal faults, the differential current I_{diff} is much higher than the biased current I_{bias} (around twice in magnitude), allowing sufficient sensitivity to be provided. For external faults or heavy load conditions, I_{bias} is large, and the characteristic would require a very large I_{diff} for the protection to operate, which the spill current does not normally reach, thereby the stability of the protection is maintained. Accordingly, the setting of the parameters $(I_{s1}, I_{s2}, k_1, k_2)$ should be carefully chosen such that both satisfactory sensitivity (against minimum-current internal faults) and stability (against maximum-current external faults) can be achieved. The minimum pick-up current setting (I_{s1}) should also consider the circuit charging current to avoid mal-operation.

In practice, it is also necessary to consider the communication delay between the differential relays to ensure that phasors that were measured at the same point in time are compared. This can be addressed by various delay compensation

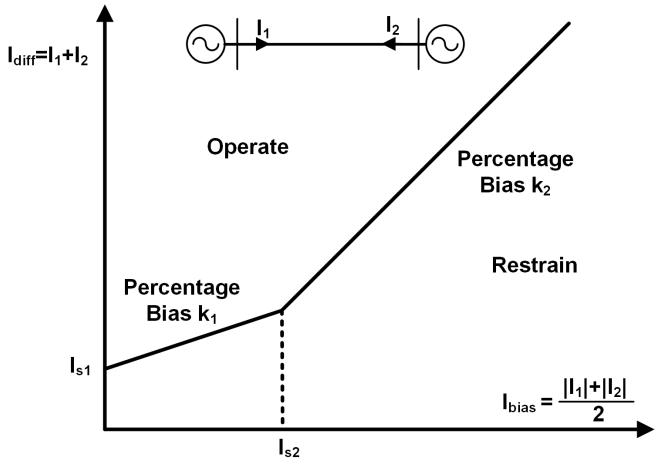


Figure 2.7: Biased characteristic of differential protection [Gri11]

methods, or by the use of accurate GPS-based time tagging of measurements at the ends of the protected zone. More details on such topics can be found in [Gri11].

2.4.2 Distance Protection

Distance protection is a form of non-unit protection, which does not independently protect a specific part of the network but provides backup by overlapping the zones of protection [Gri11]. It uses measured voltage and current to determine the impedance between the relay point and the fault. Since the impedance of the line is proportional to its length, the measured impedances can be used to indicate the distance between the relay and the fault. Distance protection schemes normally have three or more protection zones, each of which is set to a specific impedance value, which is referred as distance protection zone reach, to represent its coverage in the network. If the measured impedance is within the zone reach (with the same direction), the corresponding zone element will become active. Depending on the zone that detects the fault, different actions may be taken (e.g. issuing a trip/blocking signal) and various delays may be applied before the actions are executed.

The number of protection zone elements available is subject to the protection IED's capability, although some network operators will have a policy and may not use some of the available zones. The following provides a typical example

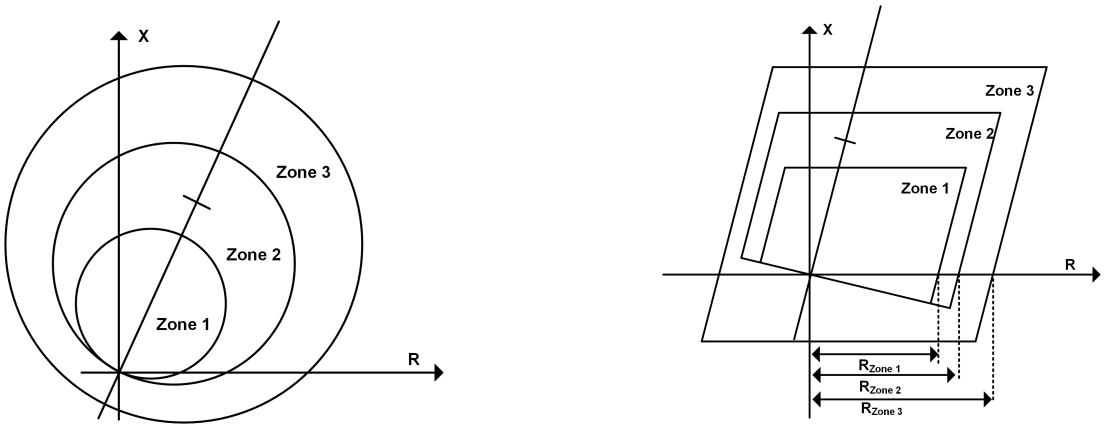
of an IED containing four protection zones, where a description of each zone is provided, along with the intended application and main considerations for the protection devices' settings.

- **Zone 1**. An instantaneous tripping zone, aiming at providing immediate clearance of faults in the protected line while avoiding mal-operation for faults beyond the protected zone. The over reaching phenomenon may be due to the inaccuracy of measurement and circuit parameters, effects from parallel circuits, etc. Therefore, it is common that a reduced value (typically 80%) of the protected line impedance is adopted.

- **Zone 2**. A delayed tripping zone that provides backup to Zone 1 and the remote end busbar protection. Typical delay is 0.5 s. The zone reach should be set to cover all faults on the protected line that are not covered by Zone 1 while see reaching beyond the remote end such that backup is provided for the busbar at the remote substation. Typically, 150 % of the protected line impedance is adopted in the GB transmission network, but it is subject to the loading condition and the elements connected to the remote end.

- **Zone 3**. An offset zone that provides delayed backup to Zone 1 and Zone 2 (on the forward direction) and backup clearance for faults at adjacent infeeding circuit and the local busbar (i.e. on the reverse direction). Typical delay applied on both directions is 1 s. The forward reach is set beyond Zone 2 reach, typically as $0.8 \times Z_1 + 1.5\%$ (in per unit value on 100 MVA base and Z_1 is the positive sequence impedance of the protected feeder). The settings should avoid the reach to the LV side (through transformers) and load encroachment. The reverse reach is normally set as 10% of the forward reach. In some IEDs, such as [Als11b], the offset characteristic can be provided by a separate protection zone.

- **Zone 4**. A reverse-looking zone used for the blocking of the remote end Zone 2 over-reach when required. It is not a tripping zone and the reach is normally set to cover all impedance seen by the remote end Zone 2 element.



(a) Mho characteristic

(b) Quadrilateral characteristic

Figure 2.8: Distance protection characteristics

The characteristic of distance protection can be plotted using an R/X diagram as shown in Figure 2.8, where two widely used characteristics Mho and Quadrilateral (Quad) are presented. There are other distance protection characteristics such as Plain Impedance, Lenticular, etc. [Gri11]. Any fault that is seen within the protection zone boundary (i.e. circle for Mho and quadrilateral shape for Quad) will activate the corresponding zone elements. Multiple elements may be active at the same time, and will issue tripping signal according the set time delay (for tripping zones).

2.4.3 Overcurrent Protection

Overcurrent protection operates when the measured current exceeds a pre-set threshold. In the GB transmission network, overcurrent protection provides backup protection for electrical components such as overhead lines, transformers, interconnectors, etc. The operating time depends on the characteristic used and the associated settings. Definite Time (DT) and Inverse Definite Minimum Time (IDMT) are the two most widely used characteristics. DT only considers whether the measured current exceeds the threshold, and if so, the protection will operate with a fixed delay. The disadvantage of DT is that the operating time is independent of the fault current level. Even with a very large fault current, the same delay is applied to isolate the fault as the faults with small currents, which

is extremely undesirable since it may provide either relatively slow clearance for high current fault or relatively fast clearance for low current faults (or overload conditions), offering little flexibility. IDMT addresses this problem by introducing a current-dependent operating time characteristic. When the measured current exceeds the pre-set threshold, the relay will operate with a time delay that is inversely proportional to the magnitude of the fault current, i.e. the larger fault current will result in smaller operating time. Figure 2.9 shows examples of IEC standardised IDMT characteristics: Standard Inverse (SI), Very Inverse(VI) and Extreme Inverse(EI) [IEC09]. These curves are governed by equations containing coefficients with different values. An SI curve is defined by the following equation:

$$t = TMS \times \frac{0.14}{(\frac{I_f}{I_s})^{0.02} - 1}$$

where t is the operating time; TMS is the time multiplier setting; I_f is the fault current; and I_s is the current setting. The coefficient values for other characteristics can be found in [IEC09].

For the setting of IDMT overcurrent characteristic, it is important to firstly consider the curve types to be used (e.g. SI, VI, EI, etc.). For example, in the GB transmission network, the SI type is adopted for the backup transmission line protection, while VI is commonly used in the cases where the current would decrease substantially as the distance from the power source increases [Gri11]. The current setting (I_s) determines the current beyond which the relay becomes active. Therefore, it should be chosen such that minimum fault condition can be detected while remaining stable for normal operating conditions (e.g. peak load condition). Both of I_s and TMS determine the time delay for the relay to operate given a certain fault current, so the settings should ensure that the required delay is achieved under specified fault conditions. Furthermore, the settings should also consider the coordination with local and adjacent protective devices such that upstream protection devices provides back-up protection for downstream devices with suitable margins [Gri11].

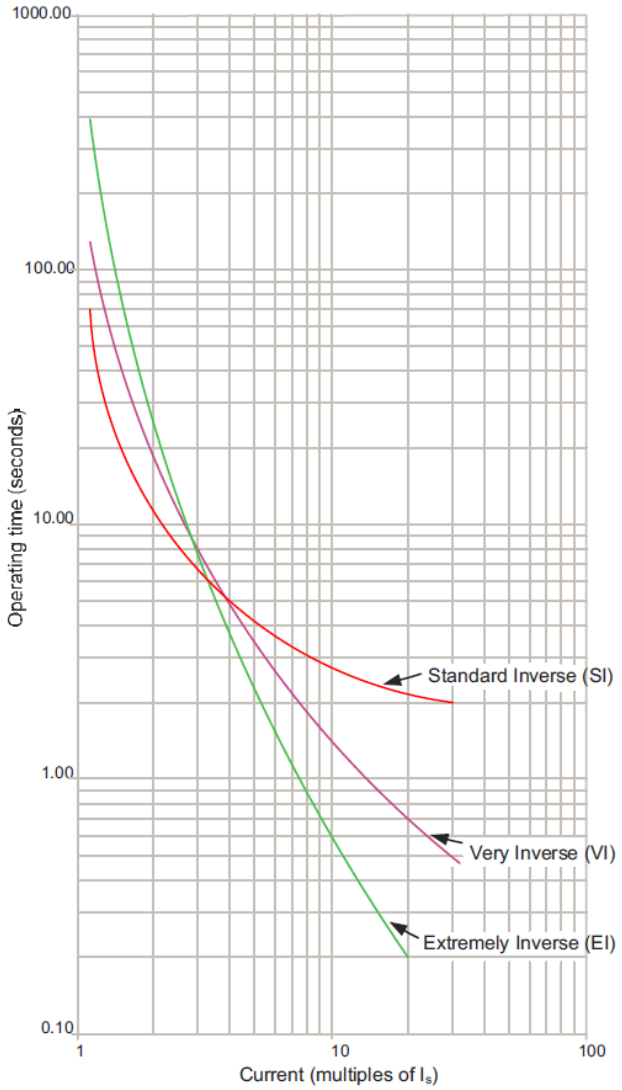


Figure 2.9: IDMT characteristics [Gri11]

2.5 Management of Protection Settings over the Life Cycle of the Application

In practice, network operators normally have their own well established process for the management of protection settings over their life cycle of application. It is important to take the setting management process into account during the design of the system for settings validation, since it will help to identify the appropriate stage(s) in the process where the validation system should be deployed, based on which optimal design can be adopted to best suit the practical needs of a particular organisation's practices.

The actual processes for settings management can be different for different network operators. Nevertheless, these approaches can be represented using a generic process as shown in Figure 2.10. Details on the specific tasks at each step are reported in [CIG13]. The whole process can be divided into the following four stages [CIG13]:

1. Preparation: this stage identifies the need for adding new devices, replacement of existing assets or the change of existing settings due to changes on the network, and the scope of the work (e.g. the new settings to be developed, the modification to be made, etc.) is identified and the associated activities are initiated.

2. Settings calculation: this stage reviews associated documents (setting policies, standards, guidance, etc.), based on which calculations of the settings are conducted including coordination studies with other protective devices.

3. Commissioning and test: this stage applies the settings to the devices and performs associated tests to ensure the settings are entered correctly and the devices will operate as expected.

4. Review and record: this stage records and stores the settings in certain formats and location for documentation purpose.

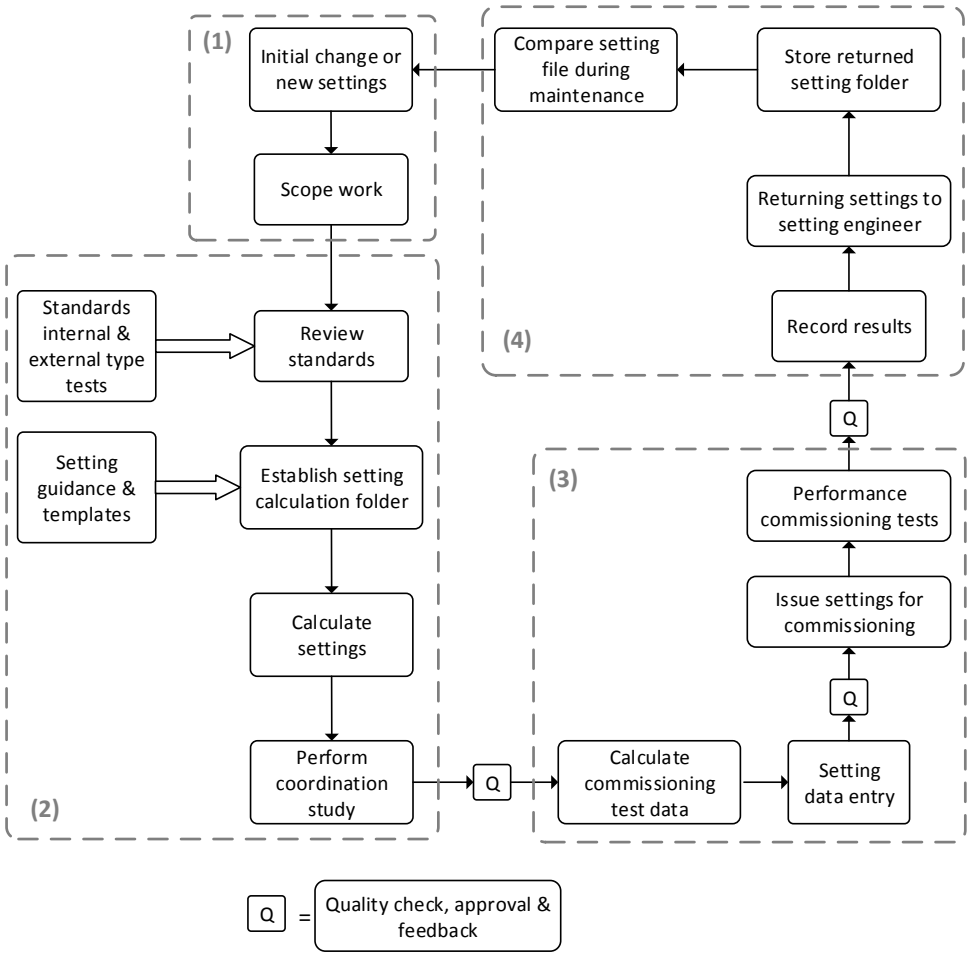


Figure 2.10: Generic process for the management of protection settings over the life cycle [CIG13]

Over the life cycle of the protection settings, multiple software tools (e.g. settings calculation tools, setting management tools, etc.) may be deployed; documents with different formats and versions may be used; and different groups of people (in-house engineers and contractors) may work on the process. Setting errors may be introduced at any stage. The main source of errors can be summarised as follows:

- Incorrect selection of solutions. This may include making mistakes in choosing protection functions for protection specific equipment (although this is rare), configuration of protection functions in a multi-function protection IED, etc.

- Calculation errors. This can be due to mis-understanding and translation of associated policies and guidance, mistakes in calculations (e.g. fault calculations), failure in finding satisfactory settings to meet associated requirements, etc.

- Mistakes in data transfer, entry and recording. During the settings calculation, the settings data may be transferred multiple times involving several engineers and setting data sheets or software tools; when the calculations are completed, the settings need to be applied to the relay and then documented. Any step of this process could suffer from human errors being introduced [SMB+10].

- Other sources of errors. This could result from any mistakes during the actual programming and implementation of settings on the device, or during testing and commission of the equipment associated with protection settings.

From the above discussions, it can be concluded that any stage in the process is potentially subject to errors. Therefore, this thesis proposes that the settings validation system should be the last line of checking of the exact settings applied to the physical devices. This is best performed in the commission and test stage,

when the setting file should be checked using the settings validations method presented in this thesis and then applied to the devices without any changes involved. However, this can be difficult in practice, since the existing protection settings are stored in proprietary files, which means that in many cases the setting file cannot be accessed readily by third party applications directly, but need to be converted to appropriate accessible file formats before the data can be read and analysed. Such inconveniences result from proprietary setting file formats, along with difficulties in manipulating settings data due to the use of proprietary data models to represent settings. This is the main motivation for the research presented in Chapter 4, where a solution to represent settings data using a standardised data model and file format is proposed to address these challenges, and a tool for conversion of settings from a range of proprietary formats to this standard format has also been developed and reported in Chapter 4.

2.6 Existing Research Activities and Commercial Systems Associated with Protection Settings

This section provides a review of research activities and commercial systems that are relevant to protection settings, including the systems that can calculate protection settings and commercial systems that can be used in some way for the purpose of settings validation. Discussion of the reasons why these techniques are not readily suitable for the entire validation task are provided.

2.6.1 Systems for Calculation of Protection Settings

Extensive research on the topic of automatic calculation of protection settings has been undertaken. It can be categorised into three main approaches: topological analysis, optimisation theory and AI [EAJMB05]. A brief review of the approaches of topological analysis and optimisation theory is provided, and a more detailed investigation and review of AI techniques is presented, as they are

most relevant to the research reported in this thesis.

In the topological analysis, linear graph theory [DRVP84, RVDP84, BS88, PPS91] and functional dependency theory [JKSD92] are used. The linear graph approach begins with a determination of the minimum set of starting relays, which are also referred as break points. The network is described using a graph where nodes are represented with vertices and lines with edges. The characteristics of the graph are then related to a number of matrices. The break points are derived from the manipulation of the matrices. The setting is firstly performed in the break points, after which the other relays are set in sequence to coordinate with their primary relays. In the work reported in [JKSD92], the concept of functional dependency is applied. Back-up relays are considered to have functional dependencies on primary relays. Such information is used for development of algorithms for the determination of break point set, which is a group of relays that should be primary set during the coordination process.

Optimisation theory is used in [CSS96, UPR97, PU01, AADK$^+$03], where the setting problem is formulated as the process to determine the optimal value of a objective function. The objective function being optimised is the operating time of primary relays while the settings are represented as the variables of the function. The optimisation technique is then applied for determination of the optimal (minimum) value of the operating time with the constraint of the settings and coordination criteria.

Although the literature referred to above describes high quality research outputs, the practical applications of such techniques are limited as only basic settings are considered in these work while in modern numeric relays there are many other settings for configuring various functions and features, which are difficult to be considered in these approaches.

Another approach that has been widely adopted for protection setting and coordination is the application of AI techniques (particularly expert systems). Early work on the employment of computer programs to reduce calculation burden dates back to the 1960s [Tsi64, R. 77]. The systems are considered not very effective due to the lack of full incorporation of experts' knowledge [LYYJ90].

A computer-aided approach has also been adopted, where interaction between the program and engineers were required to include the engineers' knowledge to the setting process [DV84]. However, the issues still remained since the programs were not designed with any inbuilt heuristic knowledge and required manual input throughout the setting process, which largely limits these systems' capability and practical applicability. Since the 1980s, the development of expert systems made it possible to integrate engineers' knowledge within computer programs, and extensive research on the application of expert systems for protection settings has been conducted. In the following paragraphs, a number of selected activities are presented.

Lee et al. conducted extensive research on the application of expert systems for setting and coordination of protective devices in both transmission and distribution networks [LYYJ90, LCAY01, LL96]. [LCAY01] proposes a method that uses heuristic rules for the setting of protective devices in distribution networks. Heuristic rules are defined and used for guiding the search of a solution that can meet both constraints from the protective devices and the coordination requirements. Protective devices are considered as pairs of backup and primary devices (e.g. relay-recloser, recloser-fuse, etc.), each of which is assigned with a certain coordination priority that is reflected in the rules. Pairs with high priority are set initially to make sure their constraints and requirements have the highest chance of being satisfied. The knowledge is also equipped to reduce the number of infeasible settings being suggested, based on information from the adjacent devices. Compared with early computer programs, which do not incorporate heuristic knowledge and may involve large numbers of trials and errors before all constraints can be satisfied, the authors claim that the use of heuristic knowledge for guided search significantly reduces the number of trials required, thus largely increases the efficiency. However, the system only considers limited number of settings and can be difficult to be applied in current practical systems where, a wide range of protection IEDs with large numbers of settings and diverse functions are increasingly being used.

In [LYYJ90], an expert system is proposed for the setting of relays in trans-

mission systems. In this work, an object-oriented (OO) approach is used, where frames containing lists of properties are used to represent relays' specification and system information. The OO approach facilitates data retrieval and manipulation, which is also used in the work reported in the thesis (through the use of Java language for implementation). The rules are translated from documented guidance and engineers' knowledge, which includes the knowledge for selecting which rules to use, knowledge relating to settings calculation and coordination, etc. The authors claimed the use of the expert system had expedited the relay setting process with increased accuracy and consistency. The shortcoming of the system, as claimed by the authors, is the lack of consideration of practical functions, e.g. the need for manual input of fault data. Similar applications of expert systems for automatic protection settings and coordination are reported in [KSK+93, KSS97]. A key disadvantage for these systems to be widely adopted in practical applications is that they only consider a certain protection function, e.g. overcurrent protection, whereas multiple protection functions may be available in a single unit in practice.

[EAJMB05] introduces a methodology for transmission system distance protection setting based on simulated events and their consequences. The proposed approach consists of two main phases. The first phase generates credible events (i.e. various faults with source impedance variation, change of load, etc.) that defines the desired boundary limits of the target relay's protection zones. For example, for the primary protection region, i.e. the protected line, the maximum and minimum impedance measured under the various events at the desired zone reach point are recorded. Based on the results of the first phase, i.e. the boundary limits of the protection zones, coordination analysis is performed (through the use of predefined coordination rules) such that actual settings (e.g. zone reach, characteristics, time delay, etc.) can be determined, which can meet the coordination requirements and the boundary limits (as defined in the first phase). The outcome of this methodology is the zone reaches, zone time delay, operating characteristics, fault detection settings and minimum relay sensitivity represented in voltage and current. The limitation of the work is the lack of the consideration of

the capability of the actual devices to be applied during the calculation process. For example, different protection devices may have different number of distance protection zones and different supported characteristics. Without incorporating such information in the calculation process, it can be difficult for optimised settings to be obtained.

Apart from expert systems, other AI techniques have also been used for the setting and coordination of protection devices. [SL00] proposes the use of evolutionary algorithm (EA) for protection settings and coordination. The operation of protection relays and other system equipment are formulated into a set of optimisation equations and constraints. The objective is to obtain a coordination solution such that minimum operating time is achieved. EA is capable of parallel search of the optimal solution for multi-variables, which in this case are relay settings. During the optimisation process, a group of setting values are generated and passed to constraints checking and objective calculation, and the results are used as the basis for the next phase generation of protection settings. Those settings with fewer constraint violations and smaller operating time would tend to survive in the EA generation process, therefore newly settings would tend to approach a solution with fewer constraints validation and smaller operating time. Normally a fixed number of generations is applied, and the number of generations required for achieving optimum relay settings are case-dependent. Although the reported work represents a novel application of AI technique in addressing the complex protection setting and coordination problem, the application of the proposed system in practice can be limited. This is because only basic settings have been considered in the work; the number of iterations required to adopt satisfactory results is case-dependent; and it is possible that after a pre-defined number of iterations, the generated settings still can not well fulfil the coordination requirements.

The above work on automatic protection setting and coordination is not readily suitable for the validation of settings, although the task is very relevant. This is because the calculated values generally are only applicable for one setting solution, and there may be a range of valid settings available. The inconsistencies

between the calculated values with the actual settings do not mean there are errors. The various pieces of other work also do not consider checks against setting policies, in which requirements of the settings under specific system conditions (e.g. minimum fault condition) are specified. The calculated values may meet the coordination requirements, but failure in meeting the requirements in setting policies is not permitted. Furthermore, for a settings validation system, it is also desired that the validity of the policies can be validated through the assessment of the actual performance of the protection system with the settings that conform to the policies. There is no provision in such any of the reviewed systems for this task.

2.6.2 Adaptive Protection Setting Systems

Research on adaptive protection setting has been increasingly conducted in recent years [OGH03, XLD94, ADB14, CBD15]. Adaptive protection dynamically selects or changes protection settings to reflect changes in the primary system conditions to ensure optimised protection performance under all scenarios. In this section, two examples of work related adaptive protection settings are presented and reviewed.

[OGH03] proposed the application of an algorithmic-knowledge-based approach for adaptive on-line setting and coordination of protection devices in meshed networks. The expert system obtains the network topology information and setting data from the SCADA system. When changes of the state of the network are detected, the system performs short-circuit calculations and verifies whether the existing settings and coordination still valid. New coordination will be carried out if mis-coordination is detected. The coordination process is performed starting with break point relays (the locations that open the mesh by minimum number of circuit breakers), and then primary and backup relay pairs are considered iteratively in sequence until a solution that satisfies the coordination criteria is found. The engineers' knowledge is translated into rules for verifying distance protection zone reaches, pickup current setting of overcurrent protection and coordination (considering the time dial of overcurrent protection).

Around 20 rules are derived. The authors claim such an adaptive scheme can reduce the operating time and number of erroneous coordination compared to fixed settings. In this work, only basic settings (e.g. distance zone reaches) are considered without detailed consideration of various protection characteristics available. This limits its practical application where various protection characteristics and features are commonly available, and therefore must be considered.

[XLD94] proposes an adaptive protection scheme for microprocessor-based distance relays so that they can respond to various network conditions while providing fastest operation and being more sensitive to faults without losing selectivity or stability. This work is proposed to address the scenario where no communication is available to provide fast inter-tripping from the remote end of the protected line. An example of the inter-tripping scheme is that if a fault is detected in zone 1 of one relay but in zone 2 of the other in a two-ended network, a signal is typically sent instantaneously from the zone 1-detecting relay to the other relay to override the zone 2 delay timer to trip as quickly as possible. This is because the fault is deemed to be located in the protected line as it is seen by both relays in the positive direction and should be isolated instantaneously [Gri11]. Various system operating conditions, such as different fault impedances and source impedances, may result in the measured fault location being different from the actual location, which may then lead to zone 1 overreach or underreach. An ideal tripping region in the impedance plane is proposed and it is defined by the measured impedance under a wide range of system operating conditions. The region is represented using a number of lines, and any faults measured in this region will be tripped instantaneously. When a change of the system exceeds a certain limit (e.g. a switching action in the system), an updated ideal tripping region will be calculated on-line to adapt to the new system condition. Through the presented methods, the authors believe a minimum margin for zone 1 setting can be achieved, thus providing larger coverage of instantaneous operation of protected line. Although such an approach may allow a fast operation for faults that were not covered by zone 1 as in conventional approaches, the potential errors from physical devices (e.g. CT and VT errors) may affect the scheme's

performance and have not been considered.

The adaptive scheme is not a comprehensive solution for validating protection settings although it has an element of settings validation involved in its operation, i.e. the detection of mis-coordination when the network changes. In addition to the reasons associated with inability to check against setting policies as stated previously, the validation of settings requires a more comprehensive process to be a practical solution, including not only the check of coordination, but also the functional configuration, the sensitivity and stability under different fault level conditions, safety margin against CT and VT inaccuracies and normal loading conditions, etc. The methods used for detection of mis-coordination normally use a single RB approach using basic rules without the validation of its actual performance during operation, so the reliability or the coverage of all scenarios that may be encountered cannot be guaranteed.

2.6.3 Existing Systems that May Be Used for Protection Settings Validation

There are existing commercial products that may be used for validation of protection settings, although their use for this purpose not have been originally intended [Ele15, ETA15, DIg11a, Sie15, A. 14]. The common characteristic of such systems is that they all provide a platform that allows modelling of power networks, along with a library of relay models that can be supplied with settings data for the simulation of their behaviour under various system conditions. Taking [Sie15] as an example, in order to perform the settings validation, the network model is created initially. The relay models are then installed with the settings applied. Various fault events are then simulated across the network and the operation of the relays is assessed.

The disadvantages of such systems for the settings validation task are:

- The network model and the relay models are normally manually created and configured, which can be very time consuming and may require significant manual input.

- The systems usually require the whole network to be built for the simulation. This provides little flexibility for scenarios when only one or a small set of relays' settings are being validated and only a small element of the network is required for the simulation. This can be addressed by a mechanism that automatically populates equivalent network models (with different levels of detail) to suit various validation needs. However, such a mechanism is currently not available.

- The systems, relying solely on simulation outputs, provide no check against settings polices.

- Most of the systems also require manually created test scenarios and analysis of simulated results, which is not only time consuming but also not fully reliable or scalable to an organisation-wide application as business as usual.

2.7 Summary

This chapter has provided a review of the fundamentals of power system protection with a focus on the topics associated with protection settings. It can be concluded that any power system is always at risk of electrical faults, which can bring significant equipment damage, system disturbances and even large area blackouts. The protection system detects and isolates the faults within milliseconds to minimise the effect of the faults. The overall reliability of a protection system can be assessed in terms of its dependability and security, which are both closely linked to protection settings. The main considerations for the settings depend on the protection functions being used, but the overarching objective is to achieve the minimum operating time and the smallest disconnected area of the primary system following a fault. The settings are normally managed by well-established standardised processes over the life cycle of the application, but any stage of this settings management process is at risk of the introduction of errors. This information on settings management is important for the design of the intelligent system for settings validation as reported in Chapter 5.

The main research activities associated with protection settings includes systems for automatic calculation of protection settings and adaptive protection schemes. It has been shown in this chapter how the reviewed related research has fundamental shortcomings - many of the developed systems are not readily suitable for the validation of settings within a practical implementation. There are existing commercial systems that have been reported and can be used for the validation of settings, but again they have limitations due to the potential need for significant manual input during the validation process. The shortcomings of these existing systems are addressed by the methodology and design approaches developed through the research reported in this thesis.

Chapter 3

Review of AI Techniques

3.1 Overview

The field of AI was initiated in the 1950s, and its primary concern is to investigate effective ways for understanding and applying intelligent problem solving, planning, and communication skills to practical problems [Lug09]. The definition of AI can vary from different perspectives, but it can be generally summarised as the field of study to make machines behave (think, reason and act) with intelligence as human beings, using computing techniques [RN10]. The gestation of AI can date back to 1943, when Warren McCulloch and Walter Pins proposed a model of artificial neurons that had computational capabilities and suggested that a properly designed network of neurons could be used for learning. In 1956, a workshop was held in Dartmouth College (US), where attempts were made to describe intelligence and learning so that machines could effectively solve problems and improve their "knowledge" over time [RN10]. The workshop led to the creation of a computer program by Allen Newell and Herbert Simon, who claimed that the program was capable of thinking non-numerically and thereby solving the venerable "mind-body" problem [RN10]. The outcome of the workshop at Dartmouth showed that the issues addressed and the methodologies used by AI cannot be classified according to any existing disciplines at that time, and therefore AI should be classed as a separate field of study and research. This marked

the formal birth of AI. Since then, AI has received considerable research attention and a number of notable successful applications [Lug09, M. 94].

From 1980, AI effectively became an industry with the successful deployment of a number of commercial expert systems, which led to significant savings for companies [RN10]. Such successes also motivated the power industry to develop and apply expert systems to address problems in its domain, such as alarm processing, fault diagnosis, service restoration and remedial action, and guidance for preventive maintenance [M. 94]. The state-of-the-art of AI covers a broad range of applications, including robotic vehicles and speech recognition [RN10]. In power industry, intelligent agent-based systems have been increasingly investigated and used in many applications, e.g. condition monitoring, power system restoration, market simulation, network control, etc. [MDC+07]

AI can be decomposed into a number of sub-disciplines concerned with different applications, which include expert systems, automated reasoning and theorem proving, modelling human performance, machine learning, game playing, natural language understanding and semantics, planning and robotics, and AI languages and environments [Lug09]. Among these application areas, expert systems use domain specific knowledge for problem solving; automated reasoning and theorem proving solves problems by considering the problems as theorems to be proved from the background information that are treated as axioms; modelling human performance aims to simulate the process that human solves problems; and machine learning is an area which targets the improvement of machines' behaviours based on previously encountered situations and experiences. In this chapter, a number of the most widely-used AI techniques in these application areas are reviewed and critiqued. This is important and relevant to the problem being addressed by the research reported in this thesis. Other techniques (e.g. game playing and AI languages and environments), are deemed to be outside the scope of the research area reported here and are therefore not considered further.

3.2 Rule-Based (RB) Systems

3.2.1 Overview

An RB expert system uses rules to represent domain knowledge for problem solving. The rules are typically in the form of "If-Then" (or "When-Then") statements, where "If" (or "When") defines the particular set of conditions or problem context and "Then" executes actions (or triggers the interrogation of other rules) in response to the specific rule's conditions being fulfilled. Figure 3.1 illustrates the general architecture of RB expert systems, which typically contain the following components [Lug09]:

- Knowledge base. This stores the rules translated or derived from domain knowledge. Usually, the knowledge base is maintained separately from the main application such that the rules can be conveniently modified and extended (ideally without changes being required to the main program).

- Knowledge base editor. Such editors are available in many expert systems to assist the maintenance of the knowledge base, e.g. adding, removing or updating the rules.

- Case-specific data. This information, stored in working memory, is associated with the case under consideration, which include the input data to be analysed (also referred to as facts), information for retrieving associated rules, conclusions, etc.

- Inference engine. This module is responsible of matching the input facts to associated rules and determining whether the rules should be fired and the sequence for the firing of rules.

- User interface. The interface is provided to facilitate the interaction between the system and the users, and can be deigned in various forms such as menu-driven, question-and-answer, graphical/touchscreen-based, etc.

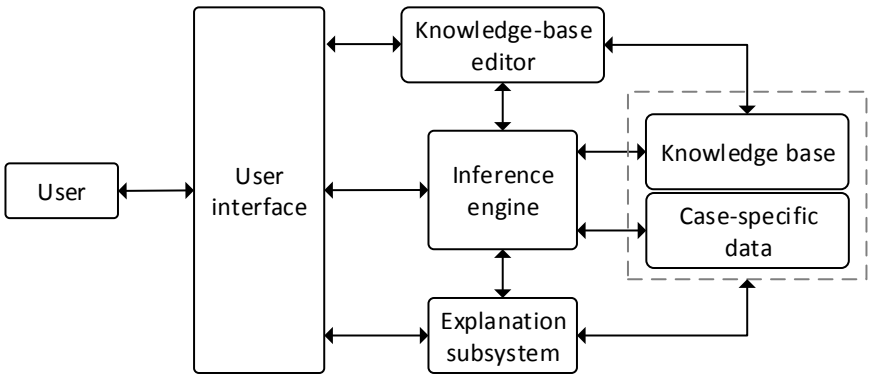


Figure 3.1: General architecture of an RB expert system [Lug09]

- Explanation subsystem. This module provides functionality for explanation of the reasoning process and to provide justifications for any conclusions made by the system.

The process to match the input facts with the associated rules in the inference engine is called pattern matching, which can be controlled according to two main strategies, i.e. forward and backward chaining.

Forward chaining is data-driven, i.e. the data are inserted into the working memory and rules are used to reason about the input data for decision-making or for drawing of conclusions. This strategy is most suitable for the situations where all preliminary facts are known [Rud10]. An example of a forward chaining engine is Drools [Red13] and an example of using Drools for implementing a condition monitoring system is reported in [RMJ10].

Backward chaining, in contrast, is goal-driven. Instead of placing facts in the working memory for reasoning, the method starts with the goal to be achieved and tries to identify the rule(s) with the conclusion that matches the goal. The conditions of the rule are then become sub-goals and matched to other rules' conclusions. The process continues to iterate until the facts that can satisfy all the sub-goals are found [Lug09]. Prolog [Bra01] is an example that uses backward-chaining for reasoning, which is used by [McA96] for protection performance assessment.

RB expert systems provide a powerful solution for the problems that previously required significant input from domain experts. The strengths of the

technique include [Lug09]:

- The ability to use domain experts' knowledge in a direct fashion, which is particularly useful in applications that rely predominantly on heuristics.
- Good explanation facilities to identify the source(s) of problems.
- Ease of deployment and flexibility for updates. The domain knowledge is mostly represented in the form of rules, making it naturally suitable to be implemented using an RB approach. The separation of the knowledge base from the reasoning engine provides the flexibility for rules to be added, removed and edited without major changes to the system.

However, RB systems also suffer from a number of weaknesses [Lug09]:

- The rules are highly heuristic but normally do not contain detailed functional knowledge of the domain.
- The system relies on the scenarios defined in the rule base for problem solving. If a novel problem instance is experienced, the system may simply fail.
- The rules translated from knowledge are usually task-dependent and offer limited reasoning flexibility, which is not consistent with human reasoning processes. The explanations often merely associate the detected symptoms with solutions, without deeper theoretical explanations being possible.

3.2.2 Application of RB Systems to Power System Protection

Following the successful application of AI techniques in various domains (e.g. medical diagnosis and chemical analysis), power engineers were motivated to apply RB expert systems for problem solving during the 1980s, and since then extensive development and application of RB systems in power systems have been undertaken [M. 94]. In the general domain of power engineering, recent application of RB systems include the analysis of partial discharge data for condition

monitoring [RMJ10], classification and analysis of power system events [SBG02], load forecasting [KEDH02], etc.

The area of power system protection has also seen extensive application of expert systems. The paper [M. 94], published in 1994, provides a detailed description of potential applications of expert systems in power system protection. Many of the specified applications have been realised, which include protection failure and event diagnosis [MDM+96, VRF+99, PWN92], protection design [BTRS94, TBRS94], protection setting and coordination [EAJMB05, LL96, LYYJ90, KSS97, KSK+93], fault diagnosis and location[KNUF92, MIK+95, FK86], service restoration and remedial action [KV91, PL97], etc. In the following paragraphs, an example RB expert systems relating to these applications is selected and presented.

Tan et al. proposed a Back-up Protection Expert System (BPES) for optimal fault clearance performance and to strive to avoid cascading outages in transmission networks [TCK+00, TCM+02]. A methodology is developed to accurately locate the fault so as to only operate the circuit breakers that are required to isolate the fault. The BPES systems are installed in substations and require the access to topology information of the protected network, the open/closed states of circuit breakers and the operational response of the existing protection relays. This information is shared among the systems through dedicated communication links. When a fault occurs, each equipment is assigned with a value called Action Factor (AF) based on the active elements of the relays that it is being protected. Active forward elements in the relays contribute positive values while active reverse elements contribute negative values. Different elements, e.g. distance protection zones, are assigned with different magnitudes of contribution based upon the coverage of their protection zone. Active primary protection zones (e.g. distance protection zone 1) are assigned with larger AF values compared to back-up protection zones (e.g. distance protection zone 2). The fault location task is achieved by the evaluation of the equipment's overall AF value using predefined rules, where the equipment with largest AF value is considered to contain the fault. Once the location of the fault is determined, BPES can identify the

minimum set of circuit breakers to open for fault isolation and send blocking signals to avoid any unnecessary trips so as to prevent cascading outages. This work represents a good attempt on addressing the potential wide-area blackouts due to backup protection. However, the authors do not seem to have considered the possibility of errors in protection settings (e.g. incorrectly configured distance zone reaches) which may lead to an incorrect AF value being calculated and result in failure to locate the faults accurately. The need for dedicated communication links for the systems that are installed in various substations may constrain their practical application due to potentially high costs.

There are also extensive applications of RB systems for assisting protection setting and coordination tasks, which are reported in Chapter 2.

3.3 Model-Based (MB) Systems

3.3.1 Overview

An MB system is a knowledge-based application where the analysis is directly founded on the specification and functionality of a physical system [Lug09]. Model-Based Reasoning (MBR) has been widely used in power system applications. A typical approach of MBR is illustrated in Figure 3.2, where the observed physical devices' behaviours (i.e. observations) are compared with the predicted behaviours (i.e. predictions) from the models. The detected discrepancies are used for the diagnosis of any failures of physical components. This approach is called consistency-based MBR. The fundamental element of any MBR system is the reasoning engine that controls the propagation of data flow through the model and compare simulated results to actual measured data [MDDM03]. The other approach is abductive-based reasoning, which uses models with fault behaviours and tests whether the abnormal operation observations align with the model-based outputs for specific problems/models. In many places, the term "MBR" is generally used to refer to the mode of consistency-based MBR [PW03], and this section adopts this convention and focuses primarily on reviewing this type

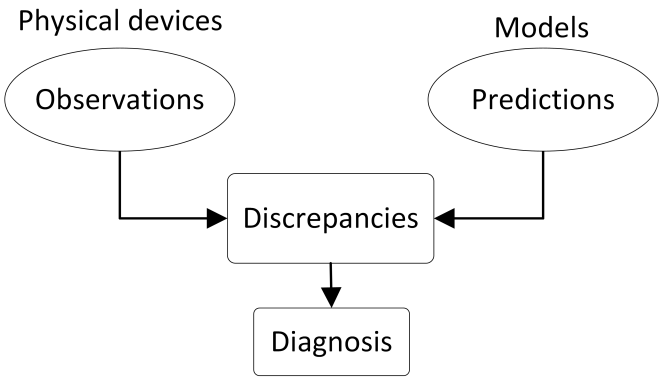


Figure 3.2: The basic principle of MBR [DMM03]

of approach.

The MBR (consistency-based) relies upon the use of models with correct behaviour, which are descriptions of physical devices/objects and their reaction to certain input stimuli. The creation of models of physical systems for qualitative simulation and reasoning requires modelling of the internal physical components, the internal structures, and the interconnections and interactions between components [Lug09].

To use MBR for diagnostic purposes, it is also required to have appropriate measurements from the physical devices (e.g observed inputs and outputs) such that actual observations can be compared to the model-generated predictions. An example of modelling of a differential protection scheme for diagnosis of protection operation is presented in Section 3.3.2.

Unlike RB approaches, which define causes and their corresponding effects in the knowledge base, the models contain the causal and structural information of physical devices, which allows them to react to a wide range of input stimuli, including those that were not anticipated during implementation. Therefore, it is considered to offer higher reliability than RB systems which may simply fail if a problem instance is not defined [Lug09]. With detailed functional knowledge inbuilt within models, MB systems are particularly useful in scenarios that involve complex interactions among multiple components. Once the models are created, they can be reused so that the effort to apply MBR for diagnosis can be minimised. In the domain of power system protection, models of equipment such as feeders,

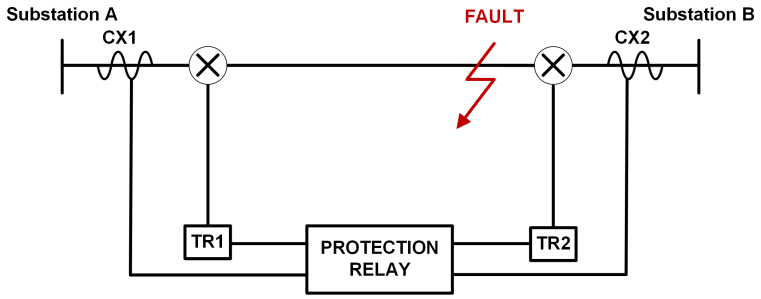
transformers, and protection relays are available in many commercially available software packages. The work reported in [MDDM03, DMM03] proposed a toolset that allowed the application of existing models for various tasks in the power engineering domain.

3.3.2 Application of MB Systems to Power System Protection

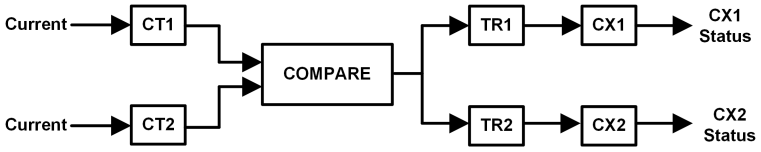
As discussed in Chapter 2, there are a number of commercially available MB systems [Ele15, ETA15, DIg11a, Sie15, A. 14] that can be used for the purpose of validation of protection settings. The common shortcoming of these systems is the potential requirement for significant manual input for tasks such as constructing network models and analysing the simulation results. These systems, although have some weaknesses for the settings validation task, are widely used for simulating the behaviours of protection systems to assist the analysis and understanding of protection functions. A methodology is proposed in Chapter 5 that avoids such laborious manual process, and in the proposed approach the principle of MBR is adopted.

MBR has been used in power system protection applications for automatic analysis of protection operation [MDM$^+$96, BMM$^+$98], alarm processing [EDM$^+$13], fault location [BDF$^+$93], fault diagnosis [LFST94], etc. In this section, an example of MBR system is reviewed and examined for investigation of how the reasoning process can be performed automatically.

Reference [MDM$^+$96] reports an MBR system that is integrated within an decision support system (DSS) for validation of protection operation. The DSS system contains two RB modules for alarm processing and fault diagnosis respectively. The motivation of the work is to automate the engineers' work to analyse protection operations following disturbance events (e.g. faults). In this work, the General Diagnostic Engine (GDE) developed by Kleer and Williams [KW87] is used, where the overall protection system model is developed by the interconnection of individual components' models with correct behaviours. The



(a) Unit protection scheme



(b) Model of the unit protection scheme

Figure 3.3: The modelling of a feeder unit protection scheme

authors claim that such an approach is proved to be appropriate for describing protection schemes. The consistency-based reasoning approach is applied, where the data from fault recorders (i.e. observables) is propagated through the developed protection system model and detect whether there are any discrepancies and conflicts between the observed and predicted behaviours.

Figure 3.3 shows an example on how a unit protection scheme is modelled in the presented work. The CTs are represented using a block, within which the conversion factor from primary to secondary side is defined. The COMPARE block models the relay's operation by taking the inputs from CTs and outputting a boolean value to indicate whether a tripping signal is issued or not. TR1 and TR2 represent tripping relays, which are the devices that are responsible of sending the tripping signal to circuit breakers. CX1 and CX2 model the circuit breakers' operation, where if tripping signal is received, the status would be changed to open. The diagnostic process is performed by injecting the data from fault recorders into the model, and observing the outputs at each stage. If a discrepancy is detected, a set of faulty candidates is generated based on the path the data flow propagates. For example, Table 3.1 shows the inputs and outputs that are observed during an internal fault, where it can be seen that CX2 fails to operate. The objective is to identify the component(s) that leads to

the operation failure. The observables (i.e. the observed inputs and outputs) are propagated through the model from both the inputs and the outputs in steps as shown in Table 3.2 and Table 3.3 respectively, where the details are represented in the format: **device = predicted value (propagated devices)**.

Input to CT1 = 23400∠33.3°
Input to CT2 = 32400∠215.6°
CX1 status = OPEN
CX2 status = CLOSED

Table 3.1: The observables for the unit protection scheme

Input to CT1 = 23400∠33.3°()
Input to CT2 = 32400∠215.6°()
CT1 = 23400∠33.3°(CT1)
CT2 = 32400∠215.6°(CT2)
COMPARE = TRIP(CT1, CT2, COMPARE)
TR1 = TRIP(CT1, CT2, COMPARE, TR1)
TR2 = TRIP(CT1, CT2, COMPARE, TR2)
CX1 = OPEN (CT1, CT2, COMPARE, TR1, CX1)
CX2 = OPEN (CT1, CT2, COMPARE, TR2, CX2)

Table 3.2: Propagation of the observables from the inputs

TR1 = TRIP(CX1)
COMPARE = TRIP(CX1, TR1)
TR2 = NOT_TRIP(CX2)
COMPARE = TRIP(CX2, TR2)

Table 3.3: Propagation of the observables from the outputs

From Table 3.2, discrepancy between the actual and predicted CX2 status is detected, and the devices that the data has propagated through are recorded, i.e. < CT1, CT2, COMPARE, TR2, CX2 >. When the observables are propagated from the reverse direction (i.e. from the outputs to inputs) as shown in

Table 3.3, a conflict relating to the predicted behaviour of COMPARE block is detected, where the set of equipment involved are < TR1, CX1, TR2, CX2>. Set multiplication is performed on the two propagated device sets and the faulty element candidate sets can be produced as <CX2>, <TR2>, <COMPARE, CX1>, <COMPARE, TR1>, <CT1, TR1>, <CT2, CX1> and <CT2, TR1>, where duplicated members in each set is combined and supersets of the listed sets are discounted. Any of the adopted candidate sets can explain the failure of the protection operation. Statistical methods are applied to determine the most likely failed element(s), where failures due to single elements is considered more probable than those resulted from multiple elements.

Such a system, although it automates the task of analysing the protection operation, does not always provide an output containing information relating to the specific failed component, as shown in the example where multiple candidate sets are generated. Furthermore, only basic elements in a protection scheme have been modelled, and other elements such as communication links are not considered, which may also be responsible for certain failures. The models of the protection relays are also very simplistic and could not be relied upon to emulate performance accurately under all circumstances, therefore limiting the applicability of the tool.

3.4 Case-Based Reasoning (CBR)

3.4.1 Overview

RB systems presented in Section 3.2 solve problems through searching for matched problem instances and their corresponding solutions/conclusions in the knowledge base. Whenever the system comes across to the same problem, the reasoning process will be performed again without referring to the previous experience. This is in contrast to reality, where experts, while perhaps applying rules, would also refer to their experience to seek similar cases so that a solution can be found and re-applied to the case being encountered at the present time. When a same

or similar scenario is found, a solution can be developed based on the previous solutions without reasoning from first principles. CBR effectively adopts such an approach by introducing a memory-centred cognitive model, where past experience can be remembered and used for guiding the problem solving [Xu94]. A key component of the CBR system is the case base, which is the database of problem solutions and may be defined by experts' knowledge or may reflect results of previous search-based successes or failures [Lug09]. When a solution to a problem is found after the search of the case base, the case will be saved for reasoning future cases.

The process of CBR is illustrated in Figure 3.4 and involves the following main steps [Lug09]:

1. Using the data relating to the present case to retrieve appropriate cases from the case base. This step is performed on the basis of similarity of the available cases to the targeted problem/present case, which is determined by their common features. Indexing terms for each case are typically used, and some terms may be weighted relative to the others. For example, when a doctor diagnoses a patient, he/she would probably recall his/her experience to seek similar cases based on the observed symptoms to draw conclusions on the nature of the patient's problem. Some symptoms may be specific to a disease, so they are considered as salient features when determining the similarities.

2. Modify the retrieved case so that it can be applied in the current situation. Often the retrieved case is not a complete match, or directly applicable, to the current case, so the reasoner needs to make modifications to the case so that it can be used for the targeted problem. Taking the medical diagnosis discussed earlier as an example, the patient may have many symptoms that match to a specific disease, but there are also some symptoms of the disease not observed from the patient, or the patient may have other symptoms that are not matched to the specific disease. In such circumstances, the doctor may need to "adjust" the case in his/her mind, e.g. considering the possi-

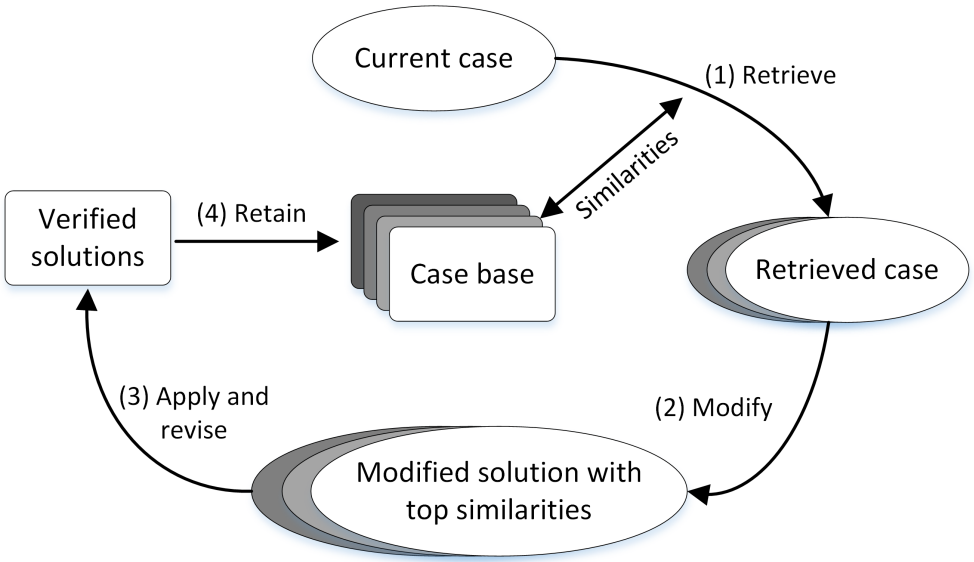


Figure 3.4: The process for CBR [AP94]

bility of existence of two diseases simultaneously or a completely different "solution", so that a solution that best matches the observed symptoms may be adopted.

3. Apply the transformed solution to the targeted problem and revise whether the solution is satisfactory or not. If not, further iteration from the previous steps may need to be performed, or a new case may have to be entered once an actual diagnosis is found if there are no cases that are applicable in the present case base.

4. Record the case for future use. The solution and the corresponding results of successes or failures are saved in the database for future cases analysis.

CBR involves representing experts' knowledge and experience relating to data and processes to learn from its experience to improve overall system performance. Therefore, CBR systems can be considered to be a combination of both expert systems [McA96] and machine learning systems [Xu94].

The advantages of using CBR include [Xu94, Lug09]:

- The system can be encoded using historical knowledge, cases and other sources directly without the need for a deep understanding of the knowledge itself. This simplifies the knowledge acquisition process and is partic-

ularly suitable for situations where a domain is not well understood or the knowledge is not complete.

- Provision of short-cuts for reasoning. CBR does not perform complex reasoning on generating a solution for the problem as is the case for RB or MB systems. If an appropriate case can be found, the problem can be solved by providing the solution directly from the previous case that matches the present case, which can be more efficient than other approaches.

Although CBR may offer compelling benefits, the downside of this technique is that there is normally not a sufficient explanation of the reasoning results when a solution is found. As the number of cases increase in the database, the time and the computation capability required to search the entire case base for a solution may also increase. Furthermore, the determination of the similarity of cases can be difficult, which may involve significant effort for the development of indexing and similarity matching algorithms.

3.4.2 Application of CBR to Power System Protection

Compared to RB and MB systems, CBR is less widely applied in the domain of power system protection. One example of the application of CBR is reported in [WSM+01b, SWM+01, WSMM01, WSM+01a], where CBR is used in the proposed Design Engineering Knowledge Application System (DEKAS) to assist the design of protection systems in transmission network. The existing approach is considered to have several shortcomings, which include difficulties in efficiently making use of experts' experience for dealing with new cases that are similar to past designs, barriers relating to knowledge and experience dissemination and the lack of a mechanism to automate the protection design process. In the reported work, the authors investigate and demonstrate the use of CBR to address these issues.

The task of designing protection systems depends on a number of factors including the network topology, the equipment being protected and the existing protection schemes in the surrounding areas. These factors are considered as

features that determine the solution (i.e. an optimum of the protection scheme design), and the cases that share similar features are considered to have similar protection requirements. These features are described using indexing parameters which are weighted based on design experts' experience that was captured and validated during knowledge elicitation sessions, where previous cases relating to design of protection systems were analysed, defined and recorded in terms of indexing features (inputs) and the ultimately-defined detailed protection design (the output). The weightings the of the indexing parameters determine the influences of the features when evaluating the similarities between the cases. Through the use of CBR, the system allows the documents and associated information from most relevant and similar cases to be retrieved and presented to the engineers, which has benefits for engineers, particularly for those who do not possess extensive experience in the design task. However, the reported work appears to require manual input to make changes to retrieved cases so that an optimised and specific solution can be obtained for the current case, and no provision appears to be made available for inclusion of new solutions within the case base automatically to extend the system's capability.

3.5 Machine Learning Techniques

3.5.1 Overview

The field of machine learning is concerned with the study of how to develop computer programs that can automatically improve their behaviours based upon prior experience [Mit97]. The capability for learning is considered to be an important property for intelligent entities [Lug09]. In order to establish such learning capability, various approaches may be taken. In this section, two of the most widely used approaches in the domain of power system protection, artificial neural network (ANN) and genetic algorithm (GA), will be investigated.

The study of ANNs is inspired by biological neural networks, which are formed by densely interconnected neurons [Mit97]. In a human brain, there are a sig-

nificant number (10^{11}) of neurons, operating in parallel [Alp10]. Each neuron is connected, on average, to 10^4 other neurons. It is this highly connected structure and the parallel processing capability that allow human brains to perform complex computations [Mit97]. The motivation for ANNs is to model the biological neural system so as to capture such powerful parallel computation and learning capabilities.

ANNs are formed by interconnected simple units referred as artificial neurons, and each unit may take a number of inputs and produces a single output. Figure 3.5 shows an artificial neuron, where x_i is the input, w_i is the weight of each input, net is the net input computed by the sum of weighted inputs, and $f(net)$ is the activation function that transforms the net input to an certain output. An ANN containing only one such unit is called a perceptron [Mit97], and it uses the threshold function as activation function, i.e. if the calculated net value is greater than a pre-defined threshold, the neuron outputs 1, otherwise -1. The learning process of a perceptron is effectively the process of adjusting the input weights and the activation function so as to provide the desired outputs. There are also other widely-used activation functions, such as piecewise-linear function and sigmoid function, which are further discussed in [AS97].

Single perceptrons can only process linear decisions, i.e. only output boolean values. For more complex tasks, e.g. speech recognition, ANNs with multilayer interconnected artificial neurons are used. A typical ANN with three layers is shown in Figure 3.6, where there is an input layer with four inputs, an output layer with two outputs, and a layer in the middle (referred as a hidden layer) with 4 neurons.

The learning process for multilayer ANNs can be performed by a number of algorithms, and the back propagation algorithm is one of the most commonly used methods [RN10]. To allow the ANNs to learn, certain amounts of training data must be available, which specifies the desired outputs given specific inputs. The back propagation algorithm calculates the errors between the actual and the desired outputs, and the errors are propagated backward to the network layers and used by a gradient descent optimisation method to find the most suitable

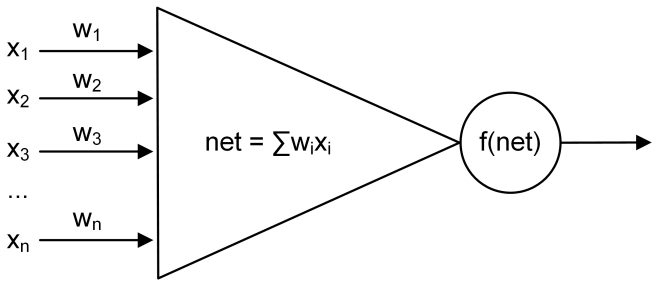


Figure 3.5: An artificial neuron [Lug09]

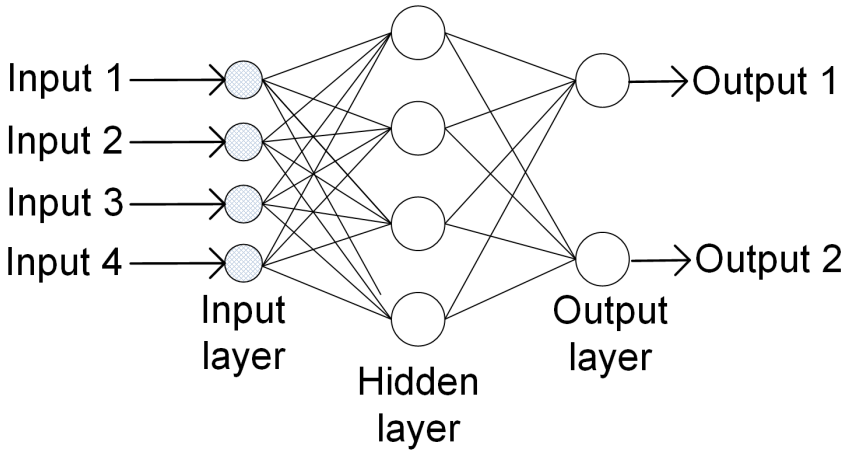


Figure 3.6: An artificial neural network [Mit97]

set of weights that can minimise the errors between inputs and desired or target output(s). When using ANNs for problem solving, it is crucial that the inputs and outputs are properly defined, which are numerical values encoded to reflect real world objects (e.g. the features or symptoms of a problem on the input and the nature/category/quantity relating to the solution on the output layer). ANNs have been very widely used in forecasting and classification applications such as forecasting of sea level [FTKM12], classifying raw data from sensors [Lug09] and face recognition [Mit97]. Recent research in this area has been increasingly focusing on the application of Deep Neural Networks (DNNs, i.e. ANNs with more than 2 hidden layers) to address complex tasks such as speech and image recognition [BS14, GB10], where improved results compared to using conventional ANNs have been observed. In the domain of power engineering, an example application of DNNs for the diagnosis of partial discharge data is reported in [CS15].

GA is another popular machine learning approach, and it is inspired by the

evolution process of human and animals, where the fittest individuals have the best chance of survival, and if they breed with other fit individuals, then even fitter offspring may be produced as the species multiples and evolves. The ultimate objective of such an approach is to populate a group of entities that can best fulfil the goal of the task in hand. A numerical term called "fitness" is typically used to measure the level of how much the entities meet the associate goal. For example, if the task is to find the best strategy for playing chess, the fitness can be defined as the number of games that an entity wins against the others among the current population [Mit97]. GA is an algorithm that allows performing this learning process, where hypotheses (i.e. potential solutions) are encoded in a form such that variations can be introduced and selection of the fittest options from within a population can be performed. Bit strings are often used for such representation purposes, and the interpretation of bit strings depends on the actual application. The learning process starts with an initial set of hypotheses, where operations such as random mutation and crossover (i.e. recombining the features of the existing hypotheses) are performed for populating the next generation of hypotheses (or candidates). At each generation, the hypotheses in the current population are evaluated using the measure of fitness, and the relatively fitter hypotheses have higher possibility to be selected as seeds for the next generation. The process is iterated until a pre-defined iteration number has been reached or a predefined satisfactory level against the goal has been achieved by the generated hypotheses. General applications of GA include learning rules for robot control, optimising circuit layout and selection of artificial neural network topology [Mit97].

3.5.2 Applications of Machine Learning to Power System Protection

The domain of power system protection has seen extensive application of machine learning techniques, including adaptive protection [Slu97], protection coordination [SL00], improving protection performance [CJ98], fault location [JBRRGM14],

etc. An overview of a system that uses evolutionary algorithm for protection coordination has been provided in Section 2.6.1.

The paper [CJ98] reports the use of ANN as an alternative computation approach to optimise distance protection performance. In this work, ANN is used as a pattern classifier, which is capable of recognising changes in power system condition (e.g. the change of the infeed to the protected circuit when a fault occurs), so as to provide more accurate zone reaches. The developed neural network is shown in Figure 3.7, where the inputs are the normalised three-phase voltage and current magnitudes measured at the busbar, and the output is the tripping decision based on the given inputs. The structure of the ANN, i.e. the number of inputs, outputs, and the layers, are determined empirically. The neural network is trained using data from simulated faults with different locations and impedance, and the back propagation algorithm has been adopted for learning. The authors claim the results show that the trained network is capable of providing very high accuracy in terms of proper trip/no trip decisions around the targeted reach point.

Although the work demonstrates effectively the use of ANNs to make decisions on whether to trip or not under various system conditions, it potentially requires a very large number of fault events to be simulated so that enough training data can be adopted for tuning the ANN to be accurate under all scenarios that may be encountered. Furthermore, the work is aimed at addressing the accuracy of zone reaches, but it appears that only zone 1 reach has been considered and the effects of CT and VT errors are not taken into account, which may affect the performance of the scheme. Additionally, if changes to the power system were made that were not in the training data, then the capability of the scheme to operate under such conditions may be questionable.

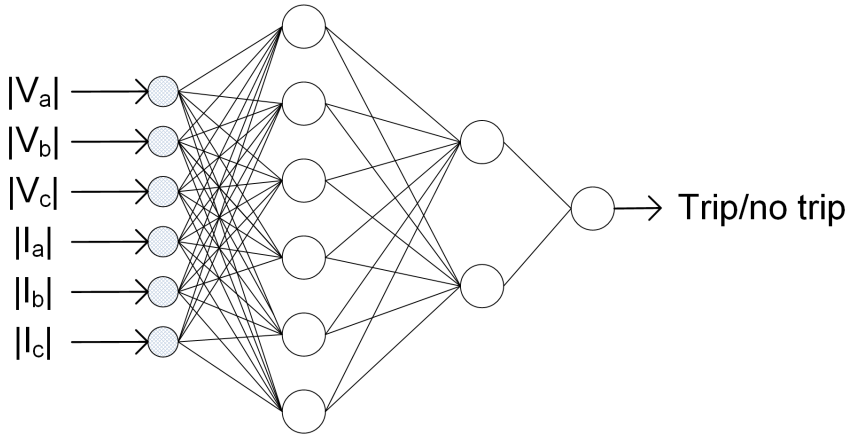


Figure 3.7: Neural network used for tripping decisions in a distance protection application

3.6 Selection of AI Techniques for the Validation of Protection Settings

In the previous sections, various AI techniques and their applications in the field of power system protection have been reviewed. The outcomes have been used for the evaluation of the most suitable approach of the validation of protection settings, which is the targeted task in this research work. A hybrid RB and MB system is considered to be capable of comprehensively performing the settings validation task and has been adopted. In this section, the reasons on why such a hybrid approach has been selected, as opposed to other available techniques/approaches, are discussed.

3.6.1 Why an RB and MB Hybrid Approach is Adopted?

In this research work, an RB and MB hybrid approach has been adopted as the solution for comprehensive validation of protection settings. The need for such a hybrid system is due to the inherent weaknesses of the selected techniques in performing the validation task, which can be complemented by the other technique's strengths. The attributes of the RB and MB approaches for the settings validation task are summarised in Table 3.4, which are discussed in detail in the

rest of the section.

	Strengths	**Shortcomings**
RB	• Naturally suitable for representing setting policies • Excellent explanation facilities • High level of automation • Flexibility to cope with updates in setting policies	• May fail if a problem instance is not defined in the rule base • Not capable of validating protection performance
MB	• Incorporation of functional knowledge of physical systems, allowing detection of problems that may not be anticipated during implementation • Capability of validating actual protection performance through simulation	• Difficulties in incorporating setting policies and knowledge during validation • Potential need for significant manual input

Table 3.4: Summary of the strengths and shortcomings of the RB and MB approaches for validation of protection settings

The validation of protection settings is conducted based primarily on the network operators' setting policies. In practice, it is mandatory that all of the configured settings conform to the requirements specified in the policies. These policies are written mostly in the style of rules, making them naturally suitable to be implemented in an RB system. Furthermore, the RB approach can offer excellent capability for explaining the output reasoning and rationale that underpins the suggested solution, providing a convenient way for engineers to quickly locate setting errors, identify the causes, and take corrective actions. The reasoning process, if implemented properly, can be largely automated with minimised requirements for manual input. The separation of knowledge storage, reasoning control processes and case-specific data provides flexibility for rules to be added, deleted and edited without affecting the overall system. Such a feature that allows flexible and straightforward rule management is important and beneficial,

since it is likely that the knowledge of settings validation will need to be updated as the network evolves in the future.

However, the main disadvantage of the RB approach is that it can only detect problems defined in the rule base, which may not cover all possible scenarios. As mentioned previously, new scenarios may also arise in the future as the network is modified. If a problem instance is not defined, the system may simply fail [Lug09]. The RB approach is also at risk of not being able to identify any shortcomings or errors in the setting policies, because the policies only specify requirements of the settings without checking the performance of the protection system. There may be scenarios during the actual operation that are not anticipated, e.g. a specific network configuration that has not been considered in the setting policies, the lack of consideration of effects of fault contributions from various connected routes, etc. These issues mean that the RB approach on its own does not offer a satisfactory solution for the settings validation task under all circumstances.

MB systems incorporate functional knowledge of physical systems and are capable of reacting to a wide range of system conditions, which offers an attractive capability for identifying problem instances (especially during operation) that are not anticipated during the system design or implementation. Such positive characteristics are very complementary to RB approaches and can address the several aforementioned shortcomings of the RB approach.

The disadvantages of MB systems are the difficulties in including the setting policies within the MB validation process. For example, it is required that the setting of feeder differential protection should be the same at all ends of circuits and the functions within the multi-functional IEDs should be configured (enabled or disabled) as required. Such checks can be difficult to be achieved solely using the MB approach, since the specific settings that are in violation of the policies may still function correctly under a wide range of fault events. As discussed previously, the checking against setting policies is more suitable to be addressed using an RB approach, hence the complementarity of the two approaches.

Consequently, a hybrid RB and MB approach has been adopted, which is shown to be capable of comprehensively performing the validation of protection

settings. The RB approach executes the validation function through rules translated from setting polices. In cases where unanticipated scenarios are encountered that are not fully defined in the rule base, the MB module is provided as a further means of performance checking to highlight any potential problems. The analysis of the simulation results can be automated with the aid of the RB approach to minimise requirements for the manual input during the validation process.

3.6.2 Other AI Techniques for the Settings Validation Task

Compared to the proposed hybrid RB and MB approach, other AI techniques, as reported in this chapter, do not offer satisfactory solutions.

ANNs are mainly used for classification and forecasting applications, and GA is most suitable for optimisation purposes. These techniques address problems with different focuses and nature from the settings validation task, so they are not suitable to the targeted application being investigated in this thesis. Furthermore, machine learning techniques generally involve changes being made to a system's behaviour based upon previous experience. In order for such system to operate as desired, a set of training data is needed, which is not readily available in the case of settings validation. In practice, it is desirable that any system performing the validation task should produce fixed outcomes when the same settings data and network data are inserted, so as to avoid confusion and clearly indicate any sources of problems or deficiencies. This can be difficult to achieve with machine learning techniques and does not add values compared to the proposed approach.

The application of CBR for the settings validation task would also be difficult. Although it is possible to define cases that specify the typical settings in the context of certain network topologies, system conditions and protected equipment, there are many more details that would need to be included in the case definition, e.g. the settings available in different relay types. Furthermore, significant effort would be required to translate the requirements specified in the policies to a range of cases, and such an approach does not offer any extra compelling

benefits compared to the proposed hybrid RB and MB approach.

3.7 Summary

AI is a broad discipline with the objective of making machines behave with intelligence in a similar fashion to human beings. Among the extensive applications of AI techniques, this chapter has reviewed the techniques that are widely applied in the areas most relevant to the research reported in this thesis. The reviewed techniques include RB expert systems, MB systems (including MBR), CBR and two machine learning techniques. Based on the outcome of the review, an RB and MB hybrid approach has been proposed which is considered to be capable of performing comprehensive validation of protection settings. The other AI techniques, while potentially being applicable to elements of the task of protection settings validation and performance checking, do not offer compelling benefits compared with the proposed approach and may require significant extra efforts for implementation and maintenance.

Chapter 4

Facilitating Settings Data Manipulation and Enabling Efficient Engineering Processes for Power Protection Systems

4.1 Introduction

To perform the validation of protection settings, one of the key steps is to investigate the methods for accessing and manipulating the settings data. Such a task can be challenging because the existing settings data are typically stored in vendor-specific proprietary formats, which require specific software tools to access. Consequently, the existing IED configuration process (an important step during the engineering of a protection, automation and control system for configuring IED functionalities, e.g. communication and protection functions) is also complex, involving multiple proprietary tools.

This chapter investigates the aforementioned issues in detail. In [HBC+13], the author proposed a solution that used the data model provided by the standard IEC 61850 [IEC10a] and its standardised System Configuration description Language (SCL) to represent protection settings. In recent years, new IEDs that

adopt the SCL format to store protection settings have been implemented [Sie13], which forms an important step towards a vendor-independent solution. However, there are still unresolved issues: 1) the automatic access and manipulation of existing proprietary protection settings data remains difficult for intelligent applications, and 2) for network operators to migrate to the new approach that is based on standardised settings, the transition process would be extremely challenging given the large amount of existing legacy data.

The key contribution of the work reported in this chapter is the design and development of an open framework to address these remaining challenges in the most effective way so as to enable efficient engineering processes and automatic analysis for protection systems. As an illustration of how such open framework can be implemented in practice, a Protection Setting Conversion Tool (PSCT) that allows automatic conversion between proprietary settings data and IEC 61850 SCL-based data has been developed and is presented. PSCT supports a number of IEDs from different vendors [ABB12, Als11b, Als11a, GE 12a] and protection schemes including distance, overcurrent, and differential. A code generation module has been developed allowing rapid prototyping of extended modules to support data conversion for new IED types and other protection functions.

The adoption of the recommendations and the methodologies presented in this chapter will facilitate the settings data manipulation for any future software applications (e.g. the settings validation system as reported in this thesis - but also other applications that require access to settings). Based on this common representation method, a novel IED configuration process is proposed, which is significantly streamlined compared with existing standardised approaches. It is shown how PSCT can be used to support the integration of legacy proprietary data to the proposed novel configuration approach.

There are a number of professional working group activities that are associated with and can be facilitated by the work presented in this chapter:

- The IEEE Power System Relaying Committee Working Group H5 (PSRC WG H5) published a report [IEE13] promoting SCL as a common format for IED configuration. A new working group, H27 (Common Format for

Relay Settings Data: COMSET), has also been started [IEE14].

- CIGRE Working Group B5.50 (WG B5.50) [G. 14] is working on a solution for vendor-independent IED configuration, which is addressed in Section 4.5.

- CIGRE WG B5.27 published a report [CIG14] on "Implications and Benefits of Standardised Protection and Control Schemes" where the standardised format of protection setting files is recommended.

- CIGRE WG B5.31 proposed potential improvements for the management of protection settings in [CIG13]. The main recommendations include: management of settings should take full advantage of IEC 61850; the engineering process should become more closely integrated with the protection setting process; improved software tools are needed to correctly, securely, and efficiently exchange and manipulate protection settings; version management of protection settings is essential; and protection settings should be capable of being accessed by various stakeholder groups.

The research presented in this chapter addresses all of the aforementioned working group activities. In particular it demonstrates steps and tools required to meet all aforementioned WG B5.31's recommendations for future protection setting management.

This chapter is organised as follows. Section 4.2 further discusses the shortcomings of the existing proprietary formats for storing protection settings. In Section 4.3, a review of the data model and the SCL format provided by IEC 61850 is presented. The methodology (as demonstrated through the implementation of PSCT) is presented in Section 4.4. The benefits and potential applications of PSCT are discussed in Section 4.5. Such benefits are demonstrated in Section 4.6 through a case study in which the PSCT is used to convert IEDs' proprietary setting files to SCL-based files for multi-vendor protection function analysis.

4.2 Existing Approaches for Protection Settings and the Shortcomings

It is reasonable to assume that, in the modern power systems engineering environment, system data should be readily accessed, exchanged, and manipulated by software applications automatically. For example, in the mobile telephony and internet industries, standards permit the exchange of texts, emails, images, videos, voice and other data between devices running different operating systems and produced by different manufactures, as well as being able to access data on one device/server from others, but this level of standardisation and interoperability is not yet apparent in the power industry. While standardised data models and formats are increasingly being used for power system data representation, storage, and exchange [IEC03, MAM+06], protection settings data are typically stored in vendor-specific formats, such as an arbitrary "binary" representation, Comma-Separated Value (CSV), and plain text. These formats are difficult to access, interchange, and manipulate automatically. Further difficulties, as reported in [A. 13a, A. 13b, AV07, IEE13, CBB+13, HBC+13, SMB+10], include: the need for vendor-specific tools to access data; the use of different data models, e.g. different representations of physical quantities and naming conventions; and different data formats used to represent the data model. Such shortcomings associated with the development of intelligent system for settings validation is further discussed in Section 4.5. The large variety of proprietary formats also presents a significant burden for engineers, who must maintain knowledge of all these formats and the associated software tools, often in an environment of increasing workloads and time pressures.

Furthermore, the existing IED configuration process (for configuring IED functions such as protection and control) based on proprietary protection settings is complex [IEC03], which involves using a vendor-independent system configuration tool and various vendor-specific IED configuration tools [HBC+13]. Consequently, multi-vendor protection, automation, and control systems are difficult

to implement and are, therefore, largely unavailable to network operators. There is a strong desire from users and stakeholders for a vendor-independent "top-down" IED configuration solution [SMB+10, G. 14, Apo05, E3 10, Bur12, X. 14a, ENT12].

4.3 IEC 61850 Data Model and the SCL Format

4.3.1 IEC 61850 Data Model

IEC 61850 is an international standard for power system automation and communications [IEC10a]. The implementation of this standard enables communications interoperability among IEDs from various vendors. A standardised data model and SCL file format are defined to facilitate interoperability across different vendors' devices. Application functions are decomposed into functional entities entitled logical nodes [IEC10c], e.g. PDIS for distance protection as shown in Figure 4.1. Within each logical node, there are data objects, which are instances of common data classes [IEC10b], to describe the functions they represent, e.g. PoRch represents the polar reach (diameter of the Mho diagram) while DirMod represents directional mode of the protection zone in a PDIS logical node. The data objects contain a set of data attributes that formally specify their details, e.g. the numerical value(s), the units, etc.

Currently, the use of data objects for protection settings within protection logical nodes is not mandatory and is not widely adopted. Although there may be concerns about the feasibility to represent protection settings using a common data model given the various proprietary functions and features available, experience of the PSRC H5 and H27 working groups' activities has revealed that the majority of existing protection functions and features can be represented using a standardised data model. The benefits of such an approach are demonstrated in the case study presented in Section 4.6.

In this work, the distance protection logical node proposed by PSRC WG

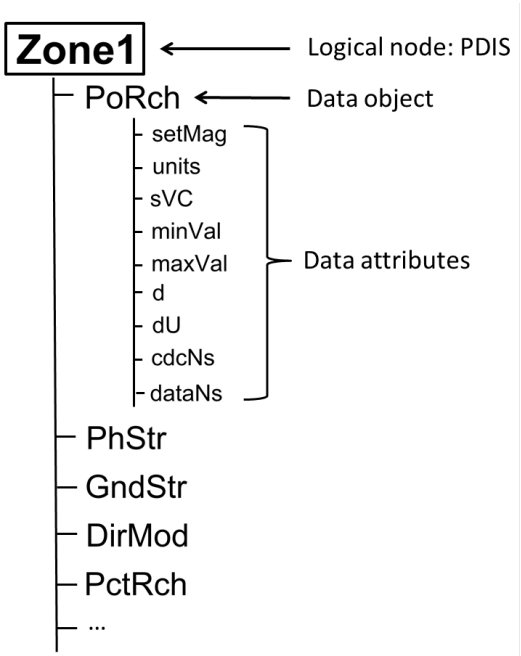


Figure 4.1: PDIS logical node in a tree representation

H5 [IEE13] and the other logical nodes defined in IEC 61850-7-4, have been adopted for the implementation of PSCT. Should the IEC 61850 standard be updated in the future with new or extended logical node definitions, a solution has been provided by introducing a code generation module that can update the PSCT to adapt to the new standard without a requirement for significant changes. Further details are presented in Section 4.4.3. For protection settings that are not currently defined in the standardised logical nodes, the information may be lost without manual intervention. However, these settings are generally associated with vendor-specific features which may not be available in other devices. Presently, the majority of the settings can be retained and are sufficient for the applications as presented in Section 4.6.

Due to the nature of protection settings, issues associated with proprietary protection functions and features must be considered. It is proposed that the standardised settings should act as a uniform interface between the internal implementation of the IED and the external applications, i.e. the implementation of the protection algorithms and logic can remain vendor-specific but standardised data model and format can be adopted to facilitate the manipulation of settings

data from external applications. The operation logic between logical nodes and the mapping of logical nodes to physical IED inputs/outputs are not defined by IEC 61850 and therefore must be specified using a vendor-specific tool. This topic is addressed in [HVNS08].

4.3.2 The SCL Format

Presently, protection setting data are typically stored in the following formats: arbitrary binary files, manually-created text files, files exported from binary files into a text- or XML-based format, and databases. SCL is a standardised file format based on XML syntax and defined in IEC 61850-6 for information exchange and description of substation functionality [IEC10a]. An IED Capability Description (ICD) file, written using the SCL, is used to indicate the logical nodes and other parameters supported by an IED. The key advantages of using the SCL format to represent protection settings, as opposed to using proprietary formats, include:

- Compared with binary files, which can only be assessed using vendor-specific software tools, the SCL format is fully documented and is openly accessible.
- An SCL-based file is formally structured and self-descriptive. Vendor-specific files may use an arbitrary representation, which varies between vendors.
- CSV is a text-based format which only directly supports flat tabular data. The description of data must be encoded in the column title or provided manually in additional written documentation. By contrast, the SCL format is semantically rich, i.e. it inherently and unambiguously defines physical quantities and units, and allows for a hierarchical data structure.
- XRIO [Omi11], based on XML syntax, is proposed for protection testing purposes. However, the representation of parameters is proprietary. In contrast, the proposed SCL format adopts an existing standardised data model, which directly provides the syntax for storing logical node parameters.

- The SCL format is part of the IEC 61850-6 standard and it provides a common format for representing a modern substation automation system [IEC03]. Therefore, protection settings data can be stored alongside the other system data presented in a SCL file, which facilities data integration.

- The SCL is formally defined by an XML schema [W3C14], which allows the validation of SCL files to be conducted automatically [BCBB13]. The generation and manipulation of an SCL file can be automatically performed by model-centric software such as the Eclipse Modelling Framework (EMF) [Ecl14b] (more details are described in Section 4.4).

4.4 IEC 61850 Protection Setting Conversion Tool (PSCT)

This section describes the design of the PSCT, which facilitates interoperability by converting from a range of proprietary formats for representing protection settings to the SCL format. The implementation of this design represents the culmination of research into how to provide protection settings data for applications such as that developed system in this research for detecting errors in setting files, but the tool is also generically applicable to any and all applications that require access to settings.

4.4.1 Overview

PSCT is implemented using the Java programming language [Ora14]. As illustrated in Figure 4.2, PSCT consists of a data translation module and a code generation module. The proprietary protection setting files are converted into standardised SCL files by the data translation module. The code generation module automatically generates codes allowing rapid prototyping the support for new IED types and protection functions while requiring minimal manual input.

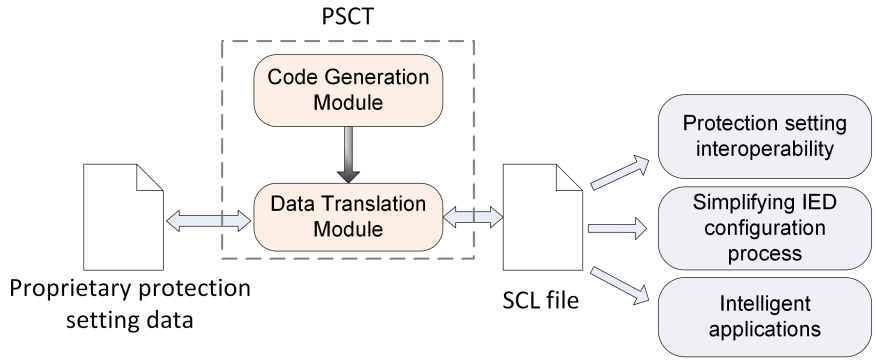


Figure 4.2: Overview of PSCT and potential applications of the translated SCL-based settings format

4.4.2 Data Translation

The data translation process shown in Figure 4.3 involves three main steps: data importing, mapping, and exporting.

4.4.2.1 Protection Setting Data Importing

The data importing step is required to access the protection settings data from the original data source for further manipulation and processing.

Binary setting files generally cannot be accessed directly without using vendor-specific tools. However, these files can normally be exported by the vendor's tool as text, typically in CSV format, or as XML files. The data importer described contains parsers that are capable of interpreting the files generated by a number of vendors' tools for IEDs [Als11b, Als11a, GE 12a, ABB12]; further details are described in [HBC+13].

For settings stored in a database, parsing is not necessary because settings can be retrieved directly in software with reference to the database schema. If the settings data resides in a source that cannot be easily parsed, the importer also supports manual input of the data, i.e. the tool provides an interface for the user to manually enter data.

The output of the importing step is a Java object representation of the required protection functions, which includes setting values.

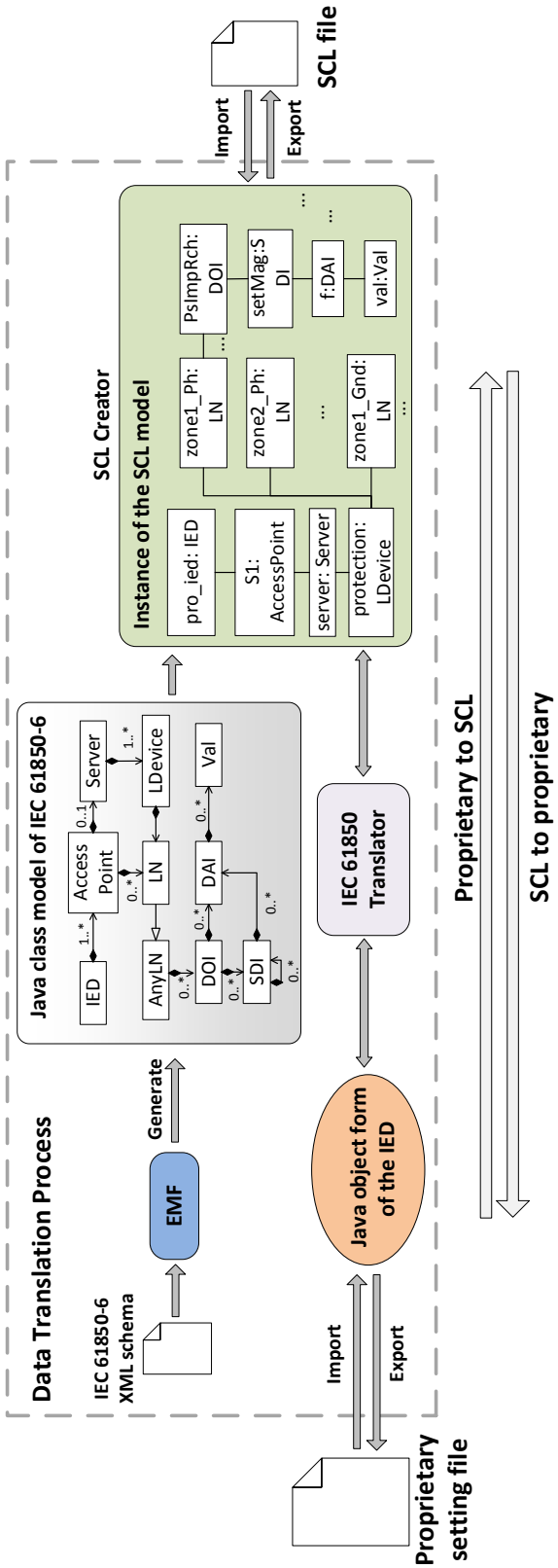


Figure 4.3: Translation process between proprietary setting formats and the SCL format

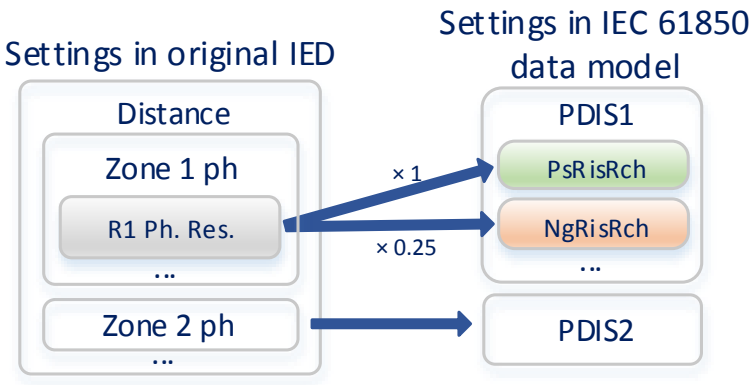


Figure 4.4: Mapping example: positive and negative resistive reach

4.4.2.2 Mapping from the Proprietary Settings to Standardised Data Objects

The mapping step is performed by the IEC 61850 Translator, shown in Figure 4.3, which contains the bi-directional mapping relations between the proprietary settings data and the IEC 61850 data objects. Figure 4.4 shows an example of mapping from the settings (represented using a proprietary format) within a commercially-available IED [Als11b] to the IEC 61850 data model. PDIS is the logical node defined in IEC 61850 to represent a distance protection zone. One distance protection zone (e.g. Zone 1 ph) is modelled using one PDIS logical node. The setting parameter R1 Ph. Res. (Zone 1 phase resistive reach) is mapped to the PDIS's data object PsRisRch (positive resistive reach). Some of the IED's specific features may not be configurable and/or visible to the user, and must be obtained manually. For example, in the original IED there is no corresponding settable parameter for NgRisRch (negative resistive reach), because the negative resistive reach is fixed at 25% of the positive resistive reach. The information therefore has to be derived from the vendor's information relating to the IED.

The building of mapping relationships between IEC 61850 data and proprietary parameters is the only manual intervention required within PSCT and is only needed once per IED type. All of the other implementation work is facilitated by a code generation module introduced in Section 4.4.3.

4.4.2.3 Exporting Protection Setting Data as SCL Files

IEC 61850-6 provides an XML schema for its data model, which defines the structure, contents, and semantics of a correctly formatted XML document [W3C14, IEC03]. As illustrated in Figure 4.3, the XML schema provided by IEC 61850-6 is used by the open source EMF software [Ecl14b] to automatically generate a Java class form of the schema. EMF is built on the Eclipse platform and is designed to facilitate the development of software based on structured models. A similar application of this tool is described in [BCBB13].

The exporting step is performed by the SCL Creator, as shown in Figure 4.3. This uses both the class structure generated by the EMF and the mapping results from the IEC 61850 Translator to create an instance of the model, i.e. it creates the relevant logical node objects. EMF also supports the automatic conversion between valid XML files and Java objects, and this feature is used by the SCL Creator to automatically export the instance of the model (in Java object format) as an SCL file (in XML format).

Validation of the generated SCL files can also be performed by importing each file using EMF, which automatically checks the syntax against the XML schema. The validator introduced in [BCBB13] performs further validation actions such as verifying the use of unique names and valid types.

An SCL file can also be converted back to a proprietary data format, so that the existing IEDs, which only support proprietary settings, can take advantage of some of the benefits of storing settings data in a common, SCL-based format. This is important for applications that require manipulating data from existing IEDs, as demonstrated in Section 4.6.

The reverse conversion can be achieved by PSCT through the following steps:

1. An SCL file is automatically imported into the PSCT using EMF, to create an instance of the SCL model.

2. The reverse mapping process is performed by the IEC 61850 Translator to create a Java form of the IED with the setting values.

3. The Java object can then be exported to any required vendor-specific format.

It is important to note that the reverse mapping process is only applicable to IEDs with the same capabilities; for IEDs with different capabilities, some information may be lost [MAE+04]. For example, if there are five instances of PDIS available within the SCL file data but the targeted IED only supports four distance protection zones, the information relating to one PDIS zone cannot be implemented by the IED without manual intervention.

4.4.3 Code Generation

Manual implementation of the translation process would require significant programming time and effort to cater for the large variety of existing IED types and protection functions. In particular, the process of creating an instance of the SCL model, which involves building the internal details of logical nodes and assigning values to the relevant data attributes, can be extremely time-consuming if performed manually. Therefore, an automatic code generation module has been developed, which significantly reduces the time and effort required to implement a translator for new IED types and protection functions.

The code generation process, illustrated in Figure 4.5, starts with a regrouping of the original IED's parameters to better match the IEC 61850 modelling approach. This process is referred to as "IED setting organization". The vendor-specific settings for different IED types may be grouped and managed in different ways and these conventions are often not well aligned to the IEC 61850 data model. For example, the distance zone reach, status and time delay settings for a given IED [Als11b] are allocated to different groups, while in IEC 61850 all such settings need to be represented in one logical node. The IED setting organisation step groups the original setting parameters into blocks that provide all the settings required by the corresponding IEC 61850-7-4 logical node, i.e. each block maps to a single logical node instance.

The result of the IED setting organisation exercise is used to initialise the

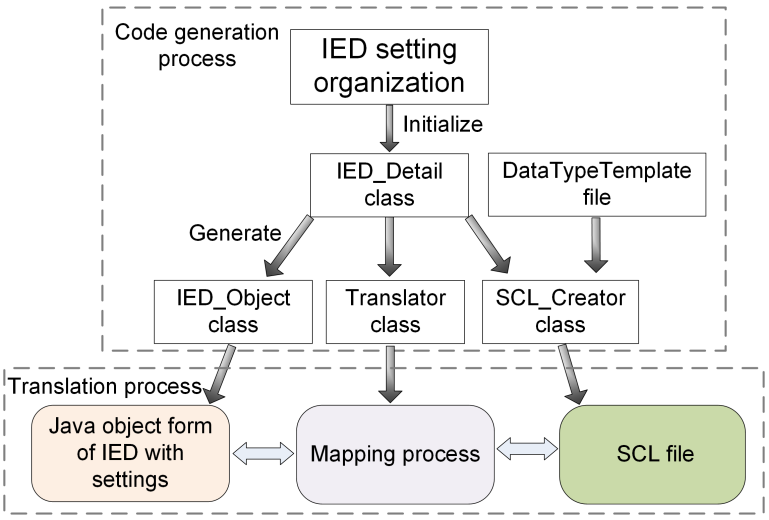


Figure 4.5: The code generation and data translation process

IED_Detail Java class, which contains detailed information about the IED, i.e. the available functions and parameters. As shown in Figure 4.5, this information is then used for generating the IED_Object and Translator classes, which are used in the data translation process to represent the IED in Java object form and to perform conversion, respectively.

The mappings between the proprietary data and the IEC 61850 data are IED-dependent, which means that any time the system is extended to incorporate settings from a new type of IED, there is a one-off requirement to manually develop the mapping relationships for that IED model. This is the only step that requires manual input during the implementation of the translation process, and the mapping development only needs to be performed once for each IED type. The code generation module automatically handles the other time-consuming and complex implementation steps, i.e. the majority of the coding work has been automatically performed.

The DataTypeTemplate file, which is a placeholder for the DataTypeTemplate section in the exported SCL file, is an XML file that contains the standardised definitions of all data types that are required by the SCL files, e.g. the logical node types, data object types, and data attribute types. This file does not need to be manually customised for each IED. The information provided by the IED_Detail object and the DataTypeTemplate file is used to generate the SCL_Creator class,

which creates an instance of the SCL model.

The key benefits of the code generation process are: it allows rapid development of a data translation process while requiring minimal manual effort; it hides the complexity of building an SCL file from the user because the hierarchical structure of the SCL model is automatically generated; and any future changes to the standardised IEC 61850 data model are reflected in the DataTypeTemplate file and the XML schema, which are both automatically utilised by the code generation module. This provides a convenient framework for updating the PSCT system over time without requiring significant effort, which is particularly useful when the existing standard is updated.

4.5 Applications

4.5.1 Facilitating Automatic Manipulation of Protection Settings

As mentioned previously, settings stored in proprietary formats bring significant challenges for software applications that require to access and manipulate the data automatically. Taking the intelligent system for the validation of protection settings being investigated in this thesis as an example, one of the elements used for validating the settings adopts an RB approach (further discussions are provided in Chapter 5). As shown in Figure 4.6, while the majority of the knowledge (stored in the setting policies) used to define the various rules remains generally similar, specific sets of rules must be defined for certain IED types due to proprietary data models used. If the setting policies are changed, it is very laborious to update the system.

Additionally, settings stored in proprietary binary files normally do not permit the access from third-party automatic applications. Accordingly, vendor-specific tools are required to export these settings to accessible file formats such as text, CSV, etc. A specific data parser is required for each IED type to extract the settings data. Each IED type also requires an specific element that contains the

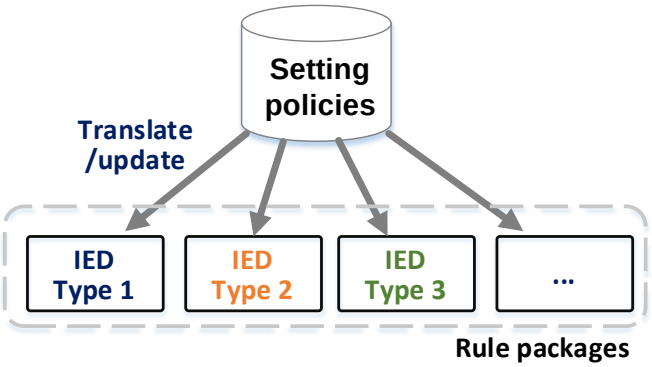


Figure 4.6: Translation of setting policies to individual IED type's rules

detailed description of the settings and function in the IED and the associated functionalities to manipulate these IED specific data. The difficulties in handling the settings data in a generic way means that continuous development is required to incorporate support for new IED types. This introduces a significant burden on the development of the tool and difficulties in maintenance of the system. All systems that may require access to and manipulation of protection settings data would suffer such difficulties.

By storing protection setting data in a standardised format, rules can be defined using a common, as opposed to proprietary, representation of protection settings. While there may still be some IED-specific features need to be considered, the number of rules that must be included is significantly reduced. Updating rules that are based on a common representation format is also much simpler, i.e. there is no need to retrospectively update rules for each IED type separately, since all IEDs utilise a single common format of input data that is independent of particular IED type/vendor. Furthermore, the task of accessing and manipulating the settings data is also significantly simplified as the data can be handled in generic manner.

The use of SCL-based setting files can be extended to many other potential applications of automatic protection system analysis and design, including: protection testing [AV07], event and disturbance analysis [A. 13b, A. 13a], protection coordination [SL00], and protection diagnostics and simulation [DMM03]. Furthermore, adaptive protection schemes would also be significantly more practical to implement with standardised settings [CBB+13].

4.5.2 Simplifying the Existing IED Configuration Process

The existing IED configuration process, as defined in IEC 61850-6, is illustrated in Figure 4.7 and involves the following steps (the numbers of the steps correspond to the numbers denoted in the figure):

1. The ICD files are generated by IED configuration tools or are retrieved from relevant databases.

2. The ICD files are imported to the vendor-independent system configuration tool together with the System Specification Description (SSD) file to carry out system level configuration, e.g. configuration of communication functions required for protection and control purposes.

3. A System Configuration Description (SCD) file is generated and sent back to the vendors' IED configuration tools for further IED-specific configuration.

4. The process of specifying protection settings is manually executed in each vendor-specific IED configuration tool and the data are saved in separate binary files and are uploaded to the IEDs.

The main disadvantage of this existing process is that it involves many steps and various software tools. Each vendor's IED configuration tool can be significantly different from the others, often requiring additional training for and experience of protection engineers. This adds unnecessary complication to the implementation of a coordinated protection, automation, or control scheme where the details of each IED type must be considered [SMB+10, Bur12, X. 14b].

To address these shortcomings, a simplified IED configuration process based on the common representation of protection settings with the aid of the proposed data conversion platform PSCT has been proposed as illustrated in Figure 4.8, which includes the following steps:

1. For legacy devices, the original setting files are translated into SCL files through the parsing, mapping and exporting process described in the pre-

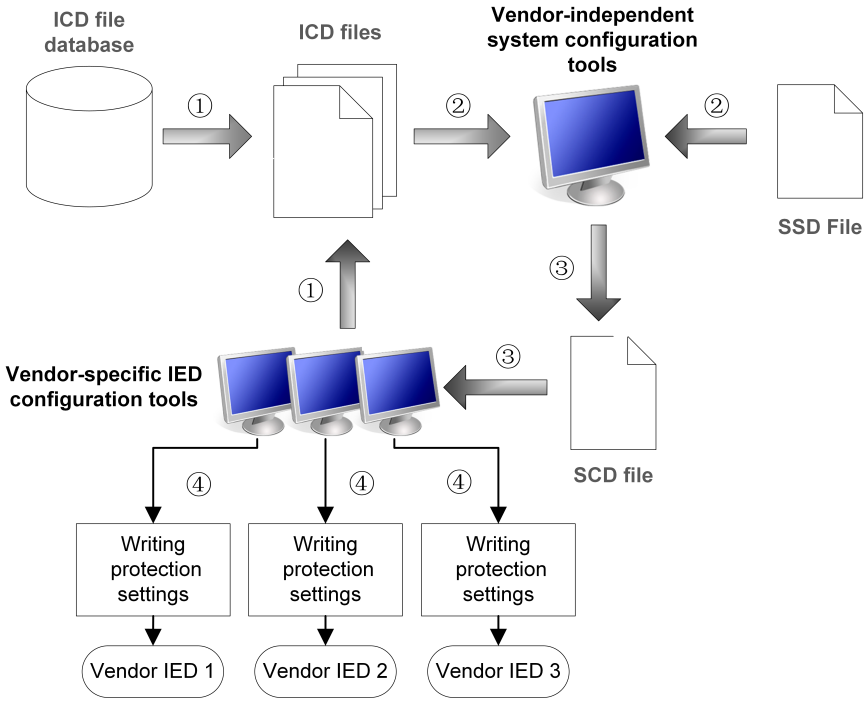


Figure 4.7: Existing IED configuration process defined in IEC 61850-6 [IEC03]

vious section. For new IEDs which support the proposed processes, this step is not needed.

2. The new ICD file is imported into the system configuration tool where the engineers configure the protection settings, if needed, at a system planning level, without considering details about which vendors' products will be used.

3. The SCD file is imported directly to each IED, and the IEDs retrieve the protection setting information from the SCD file and apply the settings automatically.

The developed approach utilises SCL-based files for the entire IED configuration process. The whole configuration process including both system-level configuration and the selection of protection settings is performed by a single vendor-independent system configuration tool. It is significantly streamlined compared with existing processes and eliminates the reliance on proprietary software. The task of configuring multi-vendor systems is thereby significantly simplified. Existing proprietary legacy data can be integrated to the process through the use

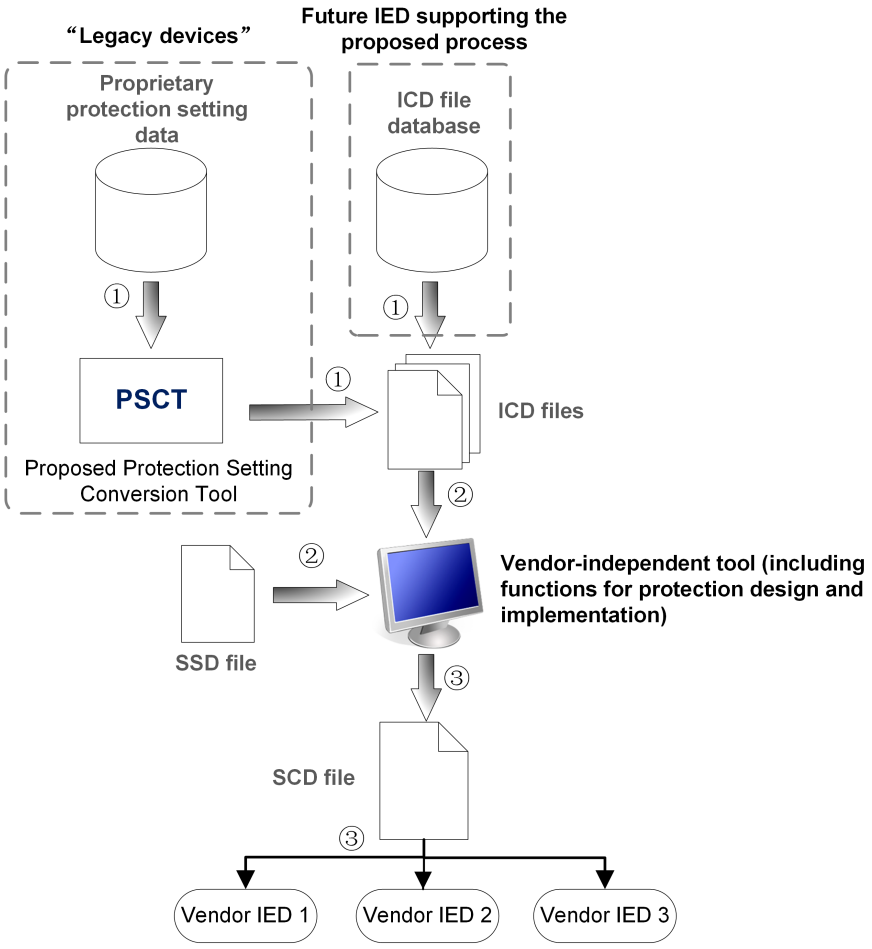


Figure 4.8: Proposed IED configuration process

of PSCT. Depending on the capability of the IEDs receiving the converted SCL-based setting data, some information may be lost or further manual configuration of the IEDs may be required (similar to the reverse mapping process described in Section 5.2).

The presented process addresses CIGRE WG B5.31's and WG B5.50's recommendations for taking full advantage of IEC 61850 for future protection setting management and vendor-independent engineering processes, including the representation of protection settings. Furthermore, the use of a common protection settings format, which is semantically well-defined and can be readily serialised to a text-based XML file, facilitates version management.

It is important to note that the proposed approach represents an ultimate goal for addressing the difficulties associated with multi-vendor systems. In the proposed process, IEDs are required to interpret protection settings from SCD files, which is not available in most existing IEDs. Although this is feasible, it potentially requires a firmware update to be issued by the IED vendors. Alternatively, vendors' IED configuration software could be updated to accept SCL-based setting files with the methodology proposed in this paper. This still requires vendor-specific software, but it avoids proprietary data formats, which would still be very beneficial to users. In any case, the work presented in this thesis supports both approaches and minimises the manual effort required.

4.6 Case Study: Multi-Vendor Overcurrent Protection Analysis

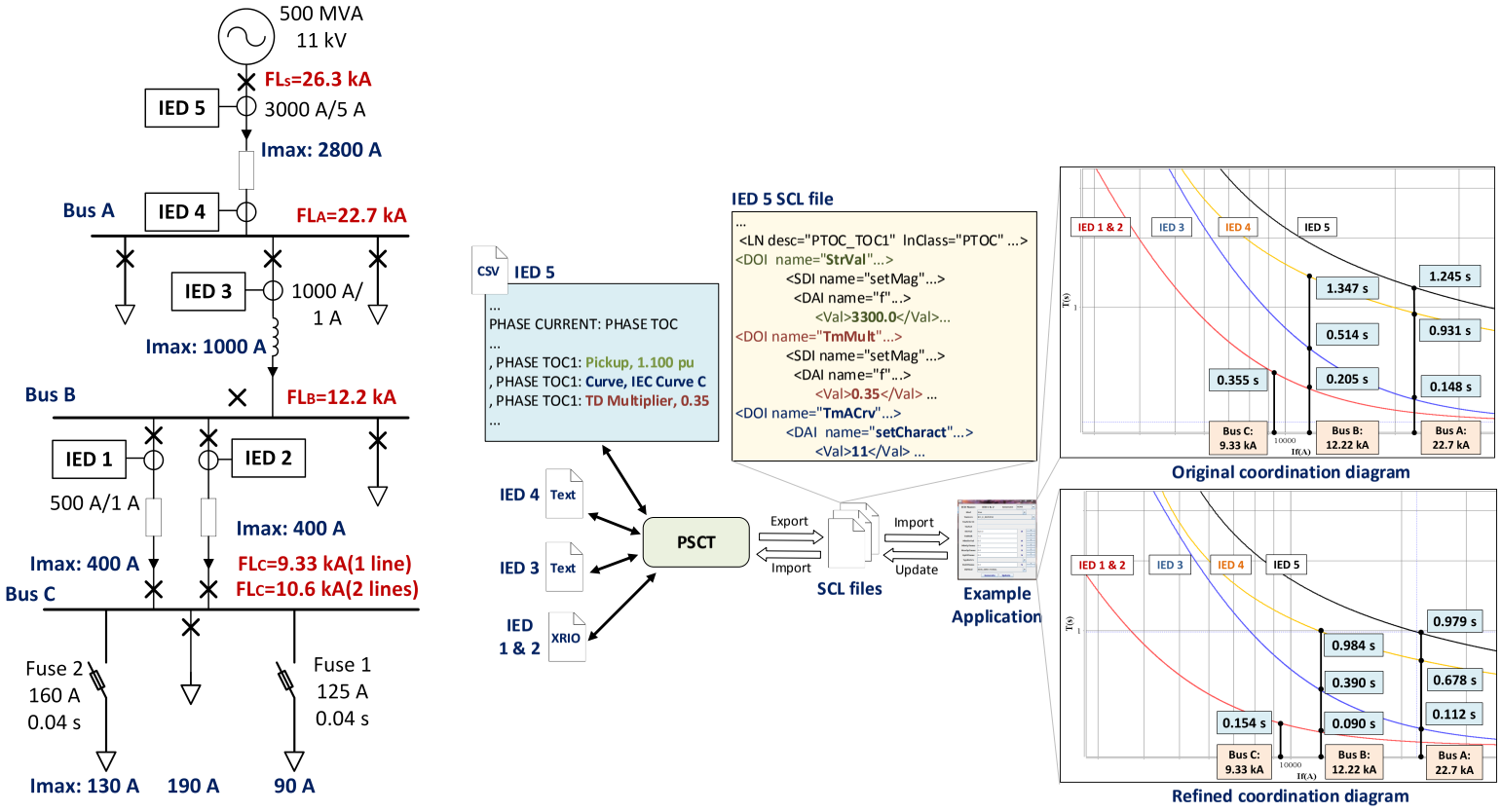
In this section, a case study is presented to illustrate the difficulties faced by software applications when attempting to automatically manipulate existing proprietary setting data. It also demonstrates how a common representation of protection settings can significantly simply the task. PSCT is used to convert existing proprietary setting files into the SCL-based setting files, which are then use for analysis of the protection function.

No.	Constraints
1	Time margin between IEDs and fuses: ≥ 0.15 s
2	Time margin between IEDs: ≥ 0.3 s
3	Current setting of IEDs: $\geq 105\%$ Max load; $\geq 3\times$ Largest downstream fuse rating.
4	IED 1, 2, 3: IEC Extremely Inverse; IED 4, 5: IEC Standard Inverse.

Table 4.1: Overcurrent coordination constraints

4.6.1 Overview

For an overcurrent protection scheme, it is important to ensure that faults are cleared within a minimum time, while maintaining coordination with neighbouring protection devices. Presently, coordination requires systematic calculation of devices' operating times for faults at various locations to check whether the coordination is achieved - although this process is often carried out in detail for a range of system conditions and then a standard "template" or "look up table" is issued for use by engineers based on the parameters of the system being protected. The process can be difficult to perform automatically due to the proprietary setting formats used. In this case study, the proprietary setting files are converted to common SCL-based files using PSCT for automatic analysis and validation of the overcurrent protection coordination. The distribution network used in this case study is shown in Figure 4.9a. There are five IEDs from three different vendors installed [ABB12, Als11b, GE 12a]. The scenario presented here is based on the example documented in [Gri11]. The coordination constraints of the overcurrent protection are summarised in Table 4.1.



(a) Case study distribution network

(b) Setting files conversion and coordination validation process

Figure 4.9: Overview of the multi-vendor overcurrent coordination demonstration

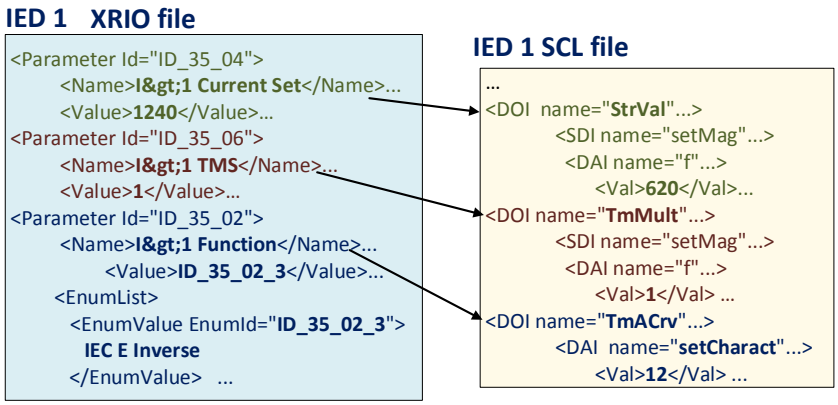


Figure 4.10: Conversion of a XRIO file to an SCL-based setting file

4.6.2 Converting Proprietary Setting Files to SCL-Based Files

As shown in Figure 4.9b, the setting data of the IEDs are stored in a number of proprietary formats represented with CSV, plain text, and XRIO. These files were imported into PSCT and converted to SCL-based files, which were successfully validated using EMF and the validator described in [BCBB13]. Figure 4.9b shows a segment of IED 5's CSV-based setting file and the resultant SCL-based file after automatic conversion. Another example is shown in Figure 4.10, which shows the conversion of IED 1's XRIO-based setting file.

It is clear that the proprietary files have different data formats and use vendor-specific data models to represent protection settings. This means that the manipulation of these files has to be performed in an IED-specific manner, which is clearly a challenge for the development and maintenance of intelligent applications. However, SCL-based settings files are readily accessible for manipulation by generic vendor-independent software. The associated mapping details of a selection of IED 1 and IED 5 settings to IEC 61850 data objects in the PTOC logical node are documented in Table 4.2 and Table 4.3.

	Proprietary		IEC 61850	
Current setting	Current Set	1240 mA	StrVal	620 A
Curve type	Function	IEC E Inverse	TmACrv	12
Time multiplier	TMS	1	TmMult	1

Note:

1) Current Set is represented in secondary value;

2) TmACrv with a value of "12" stands for IEC Extremely Inverse.

Table 4.2: Mapping of IED 1's settings to IEC 61850 data objects

	Proprietary		IEC 61850	
Current setting	Pickup	1.10 pu	StrVal	3300 A
Curve type	Curve	IEC Curve A	TmACrv	11
Time multiplier	TD Multiplier	0.35	TmMult	0.35

Note:

1) Pickup: $I_{base} = 3000A$;

2) TmACrv with a value of "11" stands for IEC Standard Inverse.

Table 4.3: Mapping of IED 5's settings to IEC 61850 data objects

4.6.3 Manipulating the SCL-Based Files for Coordination Validation and Optimisation

An example application, developed for demonstration purposes, imports the resultant SCL files and subsequently deduces the overcurrent coordination characteristics of the devices to which the data relates (this is plotted in the top-right corner of Figure 4.9b). It is shown that the coordination requirements listed in Table 4.1 have been fulfilled by the original settings. However, the operating time for IEDs 1 and 2 for a fault at Bus C is 0.355 s, which can be reduced to approximately 0.15 s through modification of settings. It is also desirable that all the curves are shifted downward for reduced operating times overall, with associated benefits to operating safety.

The settings are refined based on the common data model and the refined settings are listed in Table 4.4. The coordination diagram using the refined settings is shown in the bottom-right of Figure 4.9b which shows that coordination is maintained while the overall operating times have been reduced. The key advantage during the process is that the access to and the refinement of the settings can be performed automatically in a generic way, which is not possible to achieve with proprietary settings. Presently, the IEDs are not able to interpret these SCL files directly. Therefore, to update the IEDs' settings, the data in the SCL files are converted back to the proprietary format and applied to the corresponding IEDs manually. This step can be avoided if vendors provide new IED firmware to accept the SCL-based settings directly (as proposed in Section 4.5). Alternatively, vendors' configuration software could be updated to accept the SCL-based setting files. This still requires vendor-specific software, but it avoids proprietary data formats used in the exchange of information between individual IEDs and external software applications, which is highly beneficial from an interoperability perspective.

Developing applications that require manipulation of multiple vendors' settings files is clearly challenging. The case study shows that this problem can be addressed using the common representation of protection settings proposed in

	Original Settings / Refined Settings		
	TmAcrv	StrVal (A)	TmMult
IED 1, 2	12 / 12	620 / 480	1 / 0.724
IED 3	12 / 12	1060 / 1050	0.85 / 0.653
IED 4	11 / 11	3000 / 3000	0.275 / 0.2
IED 5	11 / 11	3300 / 3300	0.35 / 0.275

Table 4.4: Original and refined IEC 61850-based settings

this research. This provides significant benefits: convenience for network operators and system integrators, and confidence in the validity of protection settings due to the avoidance of manual input.

4.7 Conclusions

This chapter has demonstrated the use of the IEC 61850 data model and the SCL format to represent protection settings. The PSCT software allows automatic bi-directional conversion between proprietary settings data from various vendors and the proposed common format. The code generation module within PSCT provides a solution for rapid development which supports conversion modules for new IEDs and protection functions.

The advantages of using a common representation for protection settings have been demonstrated, and two potential applications and their associated benefits have been discussed. It has been shown that the SCL-based protection settings format is easier to interpret and manipulate using software (e.g. the settings validation system being investigated), which significantly reduces the burden of designing, implementing, and maintaining protection schemes. A novel IED configuration process using the proposed approach has been developed, which is streamlined compared to existing approaches. The PSCT software presented in this chapter provides evidenced supports for network operators to adopt the approach. Examples have been given which demonstrate manipulating existing protection setting data from multiple vendors, and examples of translating ex-

isting protection setting data to a common representation format have also been presented.

The work presented in the chapter addresses many recommendations for future protection setting management made by CIGRE WG B5.31. Specifically, IEC 61850 has been extended to represent protection setting data; the newly-developed IED configuration process has facilitated the integration of the protection setting process within the overall engineering process; the version management of protection settings becomes significantly easier when the data are represented in a common SCL-based format; and the protection setting conversion tool provides enhanced support for protection setting data access, exchange, and manipulation by various stakeholder applications and groups. The work also addresses IEEE PSRC WG H5, H27 and CIGRE WG B5.27's recommendations relating to the need for a common format for protection settings.

Chapter 5

A Hybrid RB and MB Intelligent System for the Validation of Protection Settings

5.1 Introduction

In Chapter 3, a hybrid RB and MB approach has been proposed for the validation of protection settings, and discussion relating to why such an approach is considered as the most effective and comprehensive solution for the settings validation task has been presented. In this chapter, details of the proposed methodology are presented and demonstrated through description of the design and operation of the intelligent system, termed PPST.

The chapter begins with an introduction of the overall design of PPST, where the functional allocation of the main components is introduced, along with a description of the process for validation of protection settings using PPST. The RB and MB modules are the two main functional elements of the overall system that perform the validation task, and the designs of these two modules are described in detail in Section 5.3 and Section 5.4 respectively.

5.2 The Overall Architecture of PPST

The overall architecture of PPST is illustrated in Figure 5.1. The system has been implemented using the Java programming language [Ora14]. PPST contains the following main elements:

- RB module: responsible for checking the settings against the rules translated from the setting policies. The module also performs automated analysis of the MB simulation results to minimise any manual input required during the MB validation process.

- MB module: responsible for performing a further means of checking of the settings using simulation-based validation, which is achieved through the interaction with the commercially available DIgSILENT PowerFactory simulation engine [DIg11a]. The original functions available in PowerFactory simulation engine are encapsulated into new functions that are specifically designed for the settings validation task, through which the population of network models, application of settings data to IED models, and creation and simulation of pre-defined fault events can be performed automatically. As noted previously, the simulation results from this module are analysed by the RB module, thus allowing the entire MB validation process to be automated.

- Data importer: the element imports network data and setting files, and stores them in the internal database for the use by other elements during the validation process.

- Database: an internal place holder for the settings data and network data.

- Graphical User Interface (GUI): this enables interaction between the users and PPST. For example, the users can input case-specific data (e.g. the protection scheme to be validated) and the system can display validation results through the GUI module. The GUI is also equipped with a graphical analysis tool that allows the viewing and graphical analysis of protection

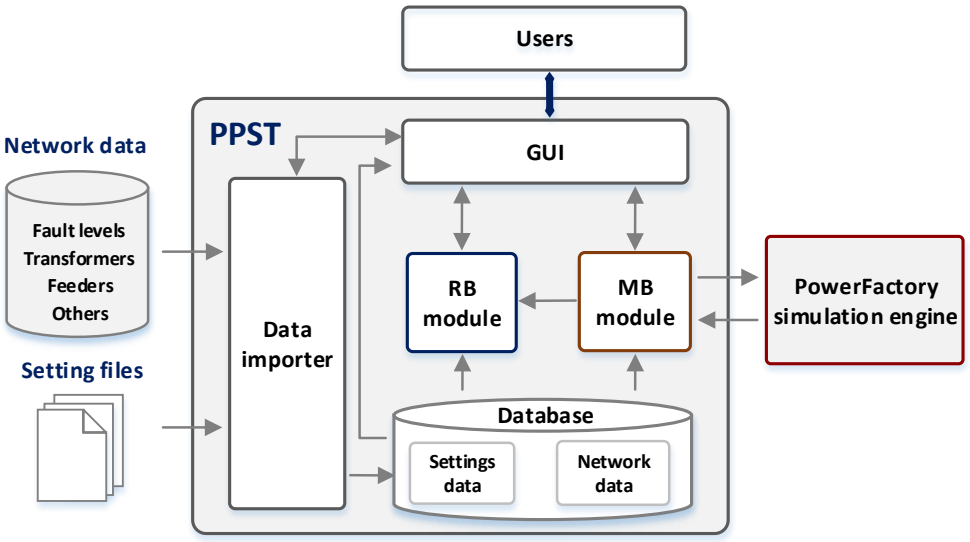


Figure 5.1: The overall architecture of the PPST

characteristics to facilitate the settings validation task. An example of the use of the graphical tool for analysing distance protection zone characteristics is presented in Chapter 6.

The validation of settings is performed on the basis of protection schemes, each of which may involve multiple protective devices. For the protection of a specific component in the network, there may be multiple protection schemes available, e.g. for feeder protection, there are differential and distance protection schemes equipped. These schemes operate independently, so they are also validated separately. Validation of the settings from a single protective device can also be undertaken, but settings are not validated against the rules that may require the access to the other protective devices' settings in the same scheme (e.g. for coordination checks). In such cases, the un-validated settings and rules are highlighted.

5.2.1 The Process of Protection Settings Validation Using PPST

The process for validation of protection settings using PPST is presented in the flow chart in Figure 5.2, and can be summarised through description of the following main steps:

1. The setting files and network data are imported to a database in PPST through the data importer, and the case-specific information (e.g. the intended protection scheme to be validated) is supplied by the users.

2. The settings data are inserted into the RB module for validation against the rules translated from the setting policies.

3. If there are any errors identified in the RB module, the erroneous settings will be highlighted, and suggestions for potential rectification of the errors are provided, along with the details of the rules that the settings violate. The generated suggestions are only for supporting decisions in settings improvement, based on which engineers may amend the setting(s) manually and repeat the RB validation process. If there is no error detected, the process will proceed to the MB stage.

4. Validation templates are retrieved by the MB module according to the case-specific information, which are then used as the basis to populate appropriate network models, apply settings to IED models, and perform simulation under various credible system events. Validation templates are defined for specific testing purposes, and contain information about the network models to be used and the fault events to be applied. Further details are provided in Section 5.4.

5. The MB results are analysed automatically using an RB approach when the simulation is complete. Such a step is to automatically identify any undesired protection operation under all of the events that have been simulated.

6. If any incorrect operation identified, it indicates that there are still remaining problems that have not been identified by the RB module, either due to deficiencies in the rule base or in the policies themselves. These problems could be setting errors, weaknesses in the protection system design, or any hidden problems during operation that have not been anticipated by the policies. In such cases, the setting policies are reviewed (manually) with the aid of generated heuristic messages about the identified undesired

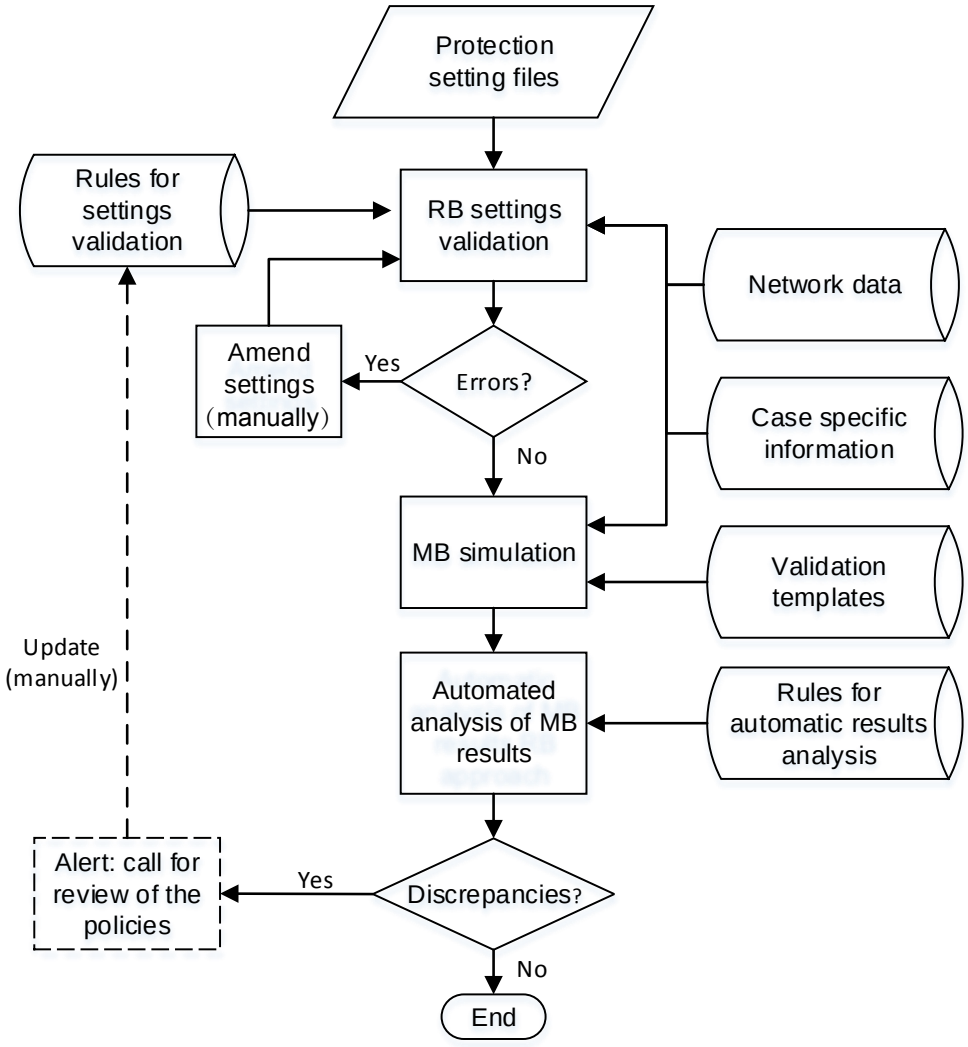


Figure 5.2: The process of validation of protection settings using PPST

operation, so that any potential weaknesses can be corrected and the missing scenarios can be added to the policies. When the setting policies are reviewed and improved, the rules for settings validation are updated for future validation.

The presented flow chart represents a default process adopted for validation of protection settings. In practice, there is no need to stop to amend settings if any errors are identified in the RB module before proceeding to MB module. Therefore, the whole process can be iterated automatically, allowing validation for large number of setting files. If errors are identified in some setting files (may be in both stages), the settings can be amended and the validation process can be

repeated. Only settings that pass the validation in both modules are considered as correct.

5.3 RB Module

5.3.1 Reasoning Strategy and Development Platform

The primary task for designing the RB module is to select an appropriate reasoning strategy (i.e. forward-chaining, backward-chaining, or a combination of the two) [Lug09]. This directly determines the platform and the associated RB inferences engine to be used for implementation and also the architecture of the RB module.

For the validation of settings, forward-chaining strategy is adopted in this work, because both settings and circuit data are known and the main objective is to draw conclusions on whether the settings are correct based on the provided data. This situation is naturally suited to the use of forward-chaining approach, which is effectively data-driven. The forward-chaining strategy is also well suited to the other main role that the RB module plays, i.e. facilitating automated analysis of the results from the MB module, where conclusions relating to the validity of protection operations are drawn based upon available simulation results data. More details on the analysis of MB results are discussed in Section 5.4.

In this work, Drools [Red13] has been selected as the platform for implementing the RB module, which provides a forward-chaining inference engine and facilities for convenient rule development and management. There are a number of benefits in using Drools as the development platform [HDB12]:

- Declarative programming and understandable rules: compared with procedural code, Drools rules are much easier for users to understand, which helps to explain the process of how a decision has been made.
- High inference efficiency: compared to other inference algorithms, ReteOO, the algorithm used by Drools, provides high efficiency in terms of matching the rules with the object data (i.e. protection settings) [Red13].

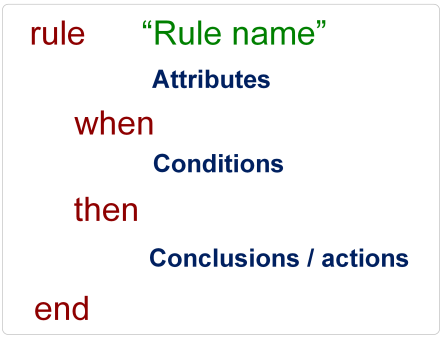


Figure 5.3: The typical structure of a Drools rule

- Ease for development and deployment: Drools can be easily integrated with other software tools such as Eclipse [Ecl14a], which provides an excellent user interface, making it much easier to edit and manage rules as well as to get immediate feedback and validation. Furthermore, Drools is based on Java, which has excellent general compatibility and interfaces, and can be run in any operating system, which is beneficial for the deployment of the system as it is not tied to a particular operating system or hardware platform.

In Drools, rules are represented in the "when-then" style as shown in Figure 5.3, where the "when" part defines the conditions for the rule to fire and the "then" part describes the actions to take or conclusions to draw when the conditions are fulfilled. A list of attributes can be defined within each rule to control the rule execution, e.g. determining the priority of the rules to fire. The rules are simply text-based files, which is easily accessible and convenient for updates.

5.3.2 The Structure of the RB Module

The overall architecture of the RB module is illustrated in Figure 5.4, where it can be seen that the rules are stored in the production memory while the input data (i.e. facts to be reasoned about) are stored in the working memory. There are mainly two types of rules that have been included in the rule base, i.e. the rules for settings validation and for MB results analysis. These rules are stored and managed separately in dedicated rule packages. When performing a certain task, only the associated rules will be invoked without affecting the others.

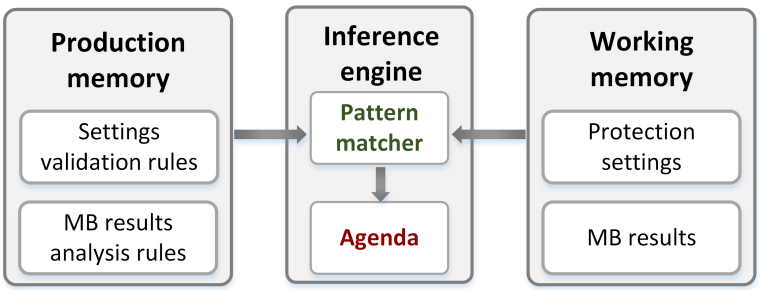


Figure 5.4: The structure of the RB module

The inference engine at the centre of the process depicted in the figure controls the rule matching and execution process. The pattern matcher (within the inference engine) matches the facts to the relevant rules according to the defined conditions. When the conditions of a rule are fulfilled, the rule will become activated. If multiple rules' conditions are met simultaneously, all of the rules will become activated and the agenda within the inference engine determines the sequence to fire the rules using a conflict resolution strategy, which can be defined by assigning salience values to the rules in their attributes or using the default last-in-first-out order [Red13].

The interaction of the production memory and working memory with the inference engine is achieved through elements called knowledge sessions. As shown in Figure 5.5, when performing a reasoning task, the rule selector retrieves rule files based on the case-specific information. For example, to select correct rule files for validating a specific protection scheme, the rule selector needs to consider the protection function being validated (e.g. differential or distance), the network topology (e.g. two-ended or three-ended), the IED type being used, etc. The retrieved rules are used for the creation of the knowledge sessions. The facts (data) are then inserted to the knowledge sessions, which interacts with the inference engine to fire the rules. Such an arrangement allows different tasks (e.g. settings validation and analysis of MB results) to be performed in different knowledge sessions independently and without affecting each other. The rules are text-based files that are stored externally to the main programs and invoked during runtime when needed, thus facilitating the rule maintaining and management.

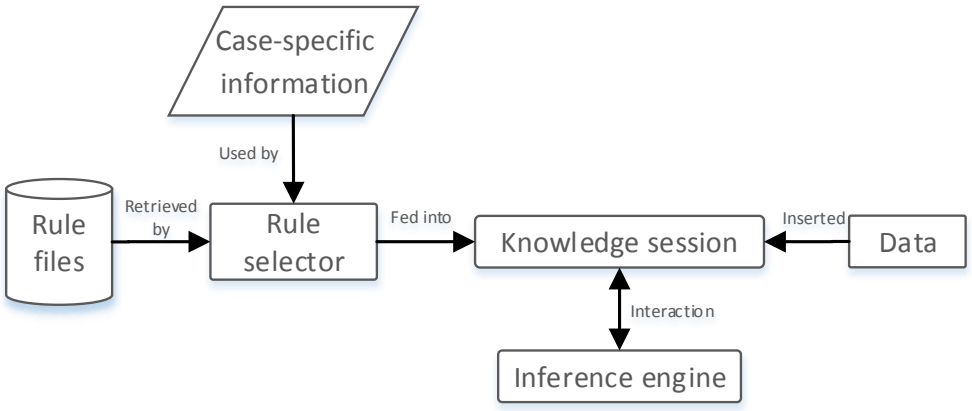


Figure 5.5: Interaction with the inference engine through knowledge sessions

5.3.3 Knowledge for Protection Settings Validation

The knowledge used for validating protection settings, as shown in Figure 5.6, has been derived mainly from network operators' setting policies and experts' understanding and experience, gathered through interviews and dialogues conducted through the research project. Such a process can be facilitated by knowledge engineering techniques and tools as discussed in [Rud10, SAA+00, SWH94].

Setting policies are a group of official documents that define the requirements relating to how the protection systems should be configured, and specify the criteria that the settings must conform to. The experts' knowledge allows the incorporation of plausibility checks, which may not be specifically defined in the policies. For example, in a certain network, the residual compensation factor (RCF) for distance earth fault protection elements tends to lie within a certain range. If the RCF is set outside the range, although it may not constitute a setting error, it is still worthwhile highlighting the situation to engineers in case there are errors that have been introduced from other sources such as erroneous circuit data. The knowledge gathered from the engineers need to be validated to ensure that it accurately reflects experts' understanding on the defined scenarios. Furthermore, a process for validating the rules translated from the setting policies and experts' knowledge is also required to make sure the rules have correctly represent the associated knowledge. These validation activities can be conducted through review meetings with experts and undertaking tests of the defined rules

under various scenarios to determine whether the rules conform to the associated knowledge.

Both the setting policies and the engineers' knowledge are generic, and further information about the protective IED is required for the rules to be developed fully. This is mainly because of two reasons: 1) the setting parameters are proprietary and the rules have to be defined over the vendor-specific settings. Such inconveniences can be addressed by the recommendations and methodologies proposed in Chapter 4 for future intelligent applications; 2) the IED itself may have specific functions and features, which need to be considered in an IED-specific manner, e.g. an IED may possess a feature that is not available in IEDs from the majority of other vendors. As shown in Figure 5.6, the IED-specific information and requirements are incorporated in the process of translation from knowledge to rules. For each IED type and each network topology, a specific group of rules are translated based on the vendor-specific settings, which can be further grouped into four categories: application, function, calculation, and coordination. The rest of the section will discuss the function of each group of rules and how they are translated from the generic knowledge. Examples of rules are provided to explain how the knowledge translation and rule development is achieved.

5.3.3.1 Application Validation Rules

The application validation rules check whether the required IEDs (i.e. with specific vendor, type, product model, firmware version, etc.) have been used for the targeted application. In practice, each protection scheme is supplied with a list of IEDs, which have been registered and comprehensively tested, and only these IEDs are allowed to be used for the specific protection task.

Although mistakes in using a wrong IED for a specific application is a highly unlikely event, failure in performing such a verification step may result in major violation of safety requirements (i.e. a situation where an IED is used that has not been comprehensively tested or approved for the specific application). Modern IEDs normally have multiple protection functions, and each IED may come with several product models and firmware versions, which can be very similar to each

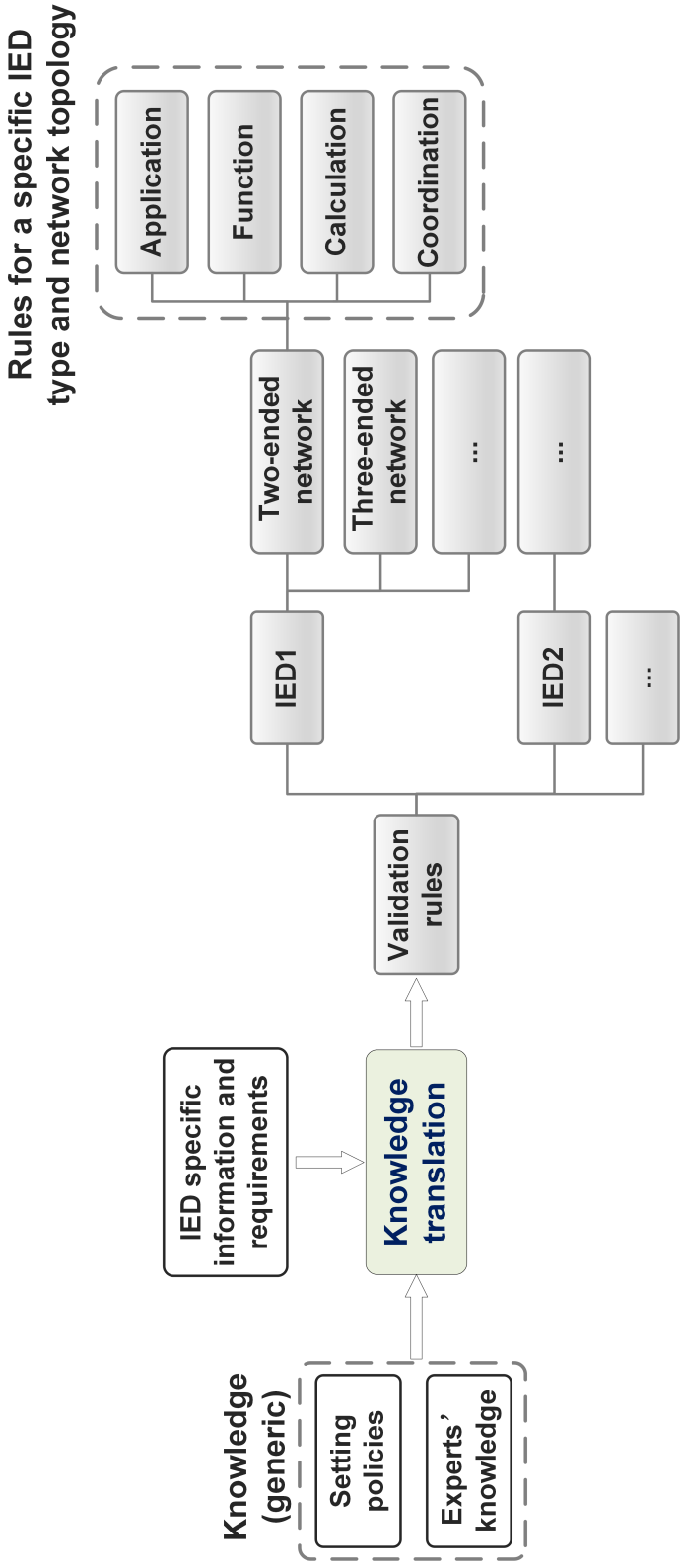


Figure 5.6: Knowledge translation and management

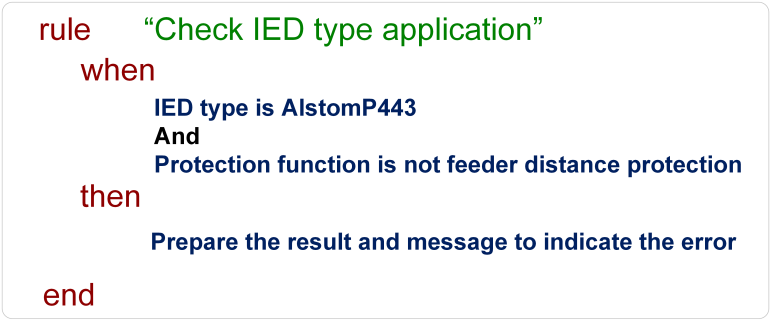


Figure 5.7: Rule for checking the application of the IED

other. These issues can contribute to a higher risk that an incorrect IED is used, especially for less experienced engineers who may not be very familiar with the devices and for network operators using new protection devices that are not very familiar to the engineers.

The current version of the prototype developed as a result of this work (as further reported in Chapter 6) enables rules to check the IED type, and further checks of the detailed product models and firmware versions can be included by introduction of additional rules in future versions of the system. Figure 5.7 shows an example rule that checks whether a specific IED [Als11b] has been used in the required protection scheme, i.e. the feeder distance protection in this case. The corresponding source code is shown in Figure 5.8. The rule initially searches for IEDs with type Alstom_P443, and if an IED is found and it is not used for the feeder distance protection, it means that the IED has been used in an incorrect application. In this example, it is assumed that the IED Alstom_P443 can only be used for feeder distance protection. The details on the error are prepared as messages in the "then" part of the rule, which are then included in the final results.

5.3.3.2 Function Validation Rules

The function validation rules are provided to interrogate the settings at the functional level, i.e. the rules check whether the functions have been configured (e.g. enabled/disabled) appropriately as required. Each IED may have multiple protection functions, but normally only a subset of the functions should be enabled for

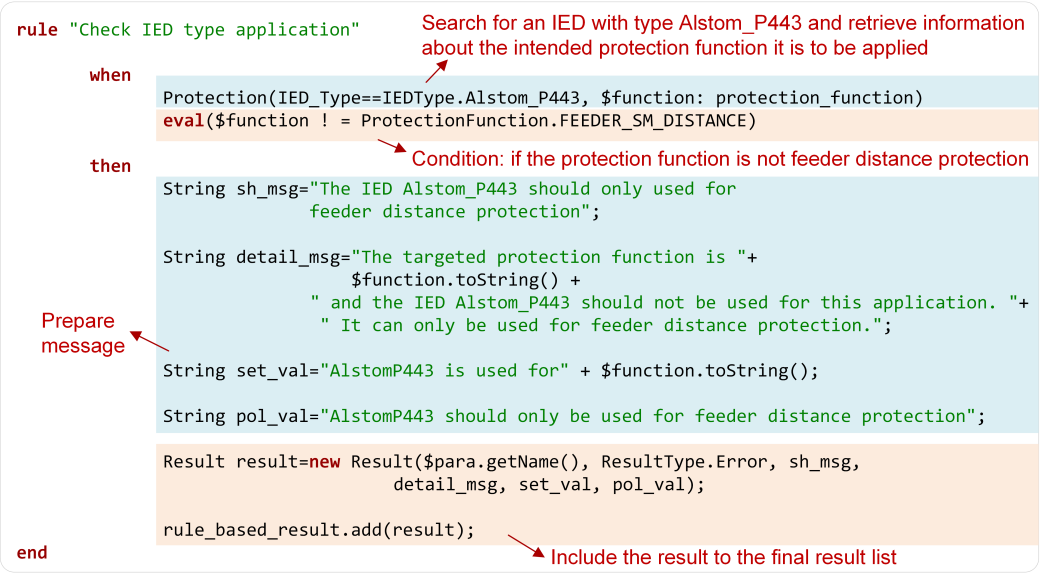


Figure 5.8: The source code for checking the application of an IED type

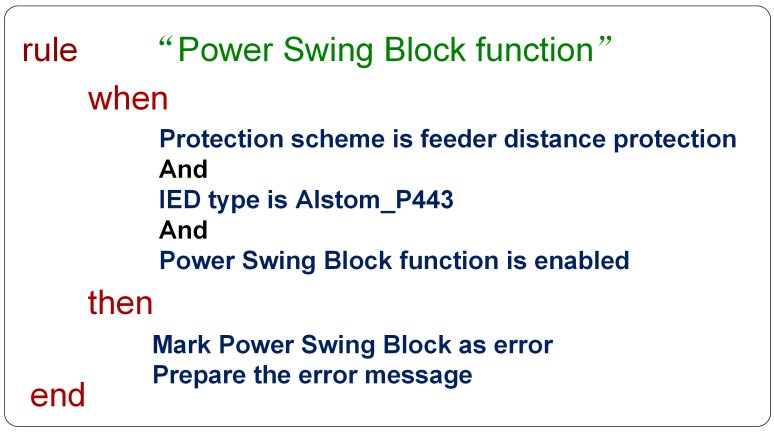


Figure 5.9: An example rule for checking the power swing blocking function configuration

a specific application. The setting policies specify the details of how the functions should be configured for each registered IED with reference to each protection scheme, which are translated as function validation rules. An example rule is shown in Figure 5.9 to check if the power swing blocking function in the IED is disabled for the feeder distance protection function as required.

Another important aspect during the function validation is the check of fixed settings. For each specific application, the network operators not only specify the standard configuration of functions, but also define a list of settings that should not be changed during the setting process unless under some exceptional

circumstances. These fixed settings are defined so that standardised solutions can be applied across the network and the values of such settings are normally not dependent on specific cases. For example, the time delay for feeder differential protection is fixed as 0 s, and this should not be changed regardless of the network topology or operating conditions. The function validation rules therefore identify the cases where the fixed settings have been inadvertently changed.

5.3.3.3 Calculation Validation Rules

The calculation validation rules are responsible for checking the settings that are configured using numeric values, such as the distance protection zone reaches and differential protection initial pick-up current setting. The translation of this type of rules involves the calculation of the optimal setting value and comparing it to the configured value. Due to the potential different calculation approaches used (e.g. different number of digits applied), it is not feasible for the configured settings to match perfectly to the optimal values as defined in the rules. To cater for such cases, certain tolerances have been applied. For example, for feeder distance protection, the setting policies require that the zone 3 resistive reach should be set as follows:

"Zone 3 resistive reach should provide maximum resistive fault coverage while avoiding load encroachment. This is achieved by selecting a resistive reach value so that 20% margin to the maximum load is provided at 30°".

Such a criterion in the setting policies can be illustrated in Figure 5.10, where R_{ch_max} is the optimal resistive reach, which can be adopted by the calculations described in Appendix B.3.4. The rules for checking such a requirement is provided in Table 5.1, where R_3 is the actual zone 3 resistive reach. In this case, a 5% tolerance is applied but only in one direction, i.e. if the configured value is smaller, but within 5% of the optimal value, it is still considered to be correct. However, the same tolerance is not applied when the setting is greater than the optimal value, since it potentially increases the risk of mal-operation rather than compromising the performance, i.e. for the zone 3 resistive reach setting, the stability of the protection function is more concerned than the sensitivity in

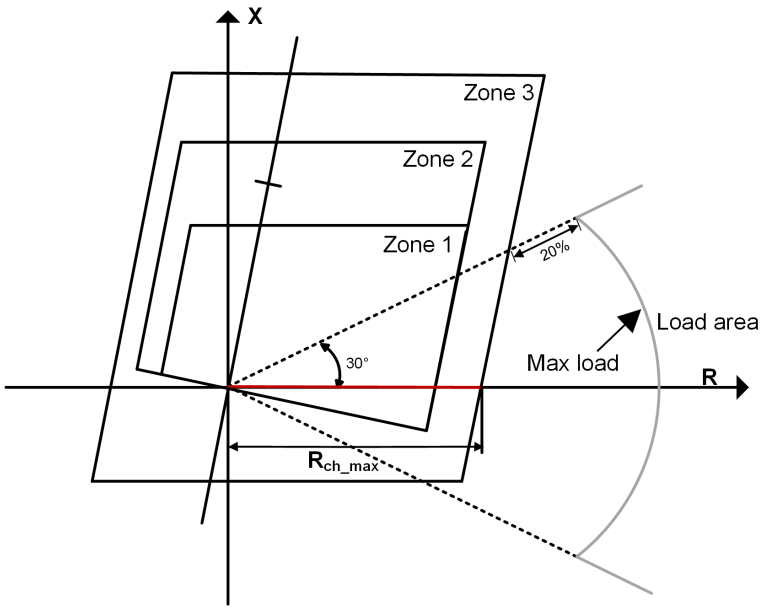


Figure 5.10: Setting of resistive reach to avoid load encroachment

this context. There are also a range of values that are defined and considered as warnings if they do not significantly deviate from the optimal values and do not lead to a higher risk of failure in operation. In this case, the range between 90% and 95% is considered as a warning level. Any values set below 90% of the optimal value are considered as errors, which must be reported and possibly addressed. The tolerance to be applied depends on the specific settings, and such information is not formally defined in the setting policies, but derived from experts' experience. A setting parameter may be subject to a number of criteria defined in the policies. It will only be designated to be correct if it complies with all requirements.

5.3.3.4 Coordination Validation Rules

The coordination validation rules contain the knowledge that defines the requirements on how the parameters should be set to properly coordinate with other protective devices within the same scheme. When performing the validation against these rules, the settings from other IEDs are required. For example, for a blocked distance protection scheme, it is required that the reverse blocking zone reach ($Zone4$) should be set as follows:

	When	Then
1	$R_3 \leq 95\% \times R_{ch\_max}$; $R_3 \geqslant 90\% \times R_{ch\_max}$	**Warning**: R_3 can be optimised by setting its value to R_{ch_max}.
2	$R_3 > R_{ch\_max}$	**Error**: R_3 is set beyond the maximum limit, which may cause load encroachment. It should be set as R_{ch_max}.
3	$R_3 < 90\% \times R_{ch\_max}$	**Error**: R_3 is set too small, failing in providing the maximum fault coverage. It should be set as R_{ch_max}.

Table 5.1: Validation rules for zone 3 resistive reach

	When	Then
1	$Z_4 < Zone4$	**Error**: Z_4 is set too small, failing in providing coverage of remote end Zone 2 reach. It should be set as $Zone4$.
2	$Z_4 > 105\% \times Zone4$	**Error**: Z_4 is set too large. It should be set as $Zone4$.

Table 5.2: Rules for validating zone 4 reach using remote end zone 2 reach

$$Zone4 = \frac{1.2 \times Zone2(Rmt) - Z_1}{0.8} \tag{5.1}$$

where $Zone2(Rmt)$ is the remote end zone 2 reach setting and Z_1 is the positive sequence impedance of the protected feeder.

The rules for checking such a criterion is shown in Table 5.2, where a 5% tolerance is applied and Z_4 is the configured value of the zone 4 reach.

5.3.4 Reasoning Process

The process of validating protection settings within the RB module is shown in Figure 5.11, and involves the following main steps:

1. Identification of the IED-specific information (e.g. IED type) from the

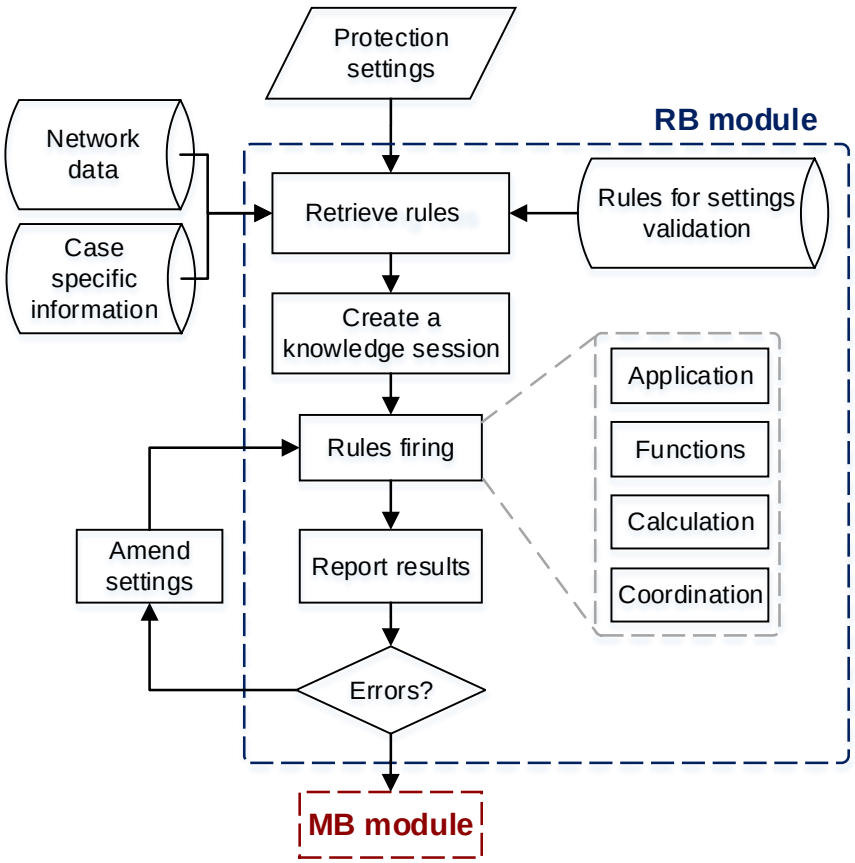


Figure 5.11: The process of RB validation of protection settings

imported setting files.

2. The IED's information, network data, and the case-specific information are utilised by the rule selector for retrieving appropriate rules for the validation task.

3. A knowledge session is created using the retrieved rules and the settings data is inserted to the knowledge session for validation.

4. The protection settings are evaluated by the rules in terms of the validity of application to appropriate protection schemes, the configuration of functions, calculations, and coordination with other protective devices.

5. The validation results are presented to the user.

6. If there are any errors or warnings identified, the users may amend the settings based on the suggestions provided and repeat the validation exercise with the amended settings. When there are no errors detected by the RB module, the settings are forwarded to the MB module for a simulation-based validation of protection performance.

5.4 MB Module

In the MB module, the principle of MBR is adopted for the validation of protection settings. A typical MBR approach, as introduced in Chapter 3, is to compare the behaviours of physical devices with simulated predictions using models, and determine any physical components' failure or degradation through detected discrepancies between observations and predictions.

In the case of protection settings validation, as shown in Figure 5.12, protection settings are applied to the IED models that are interfaced with the appropriate power network models, and a series of faults are simulated under a wide range of scenarios. The simulated results are referred to as observations, which are compared to expected protection behaviours (referred as expectations). Any discrepancies between the observations and the expectations indicate the existence

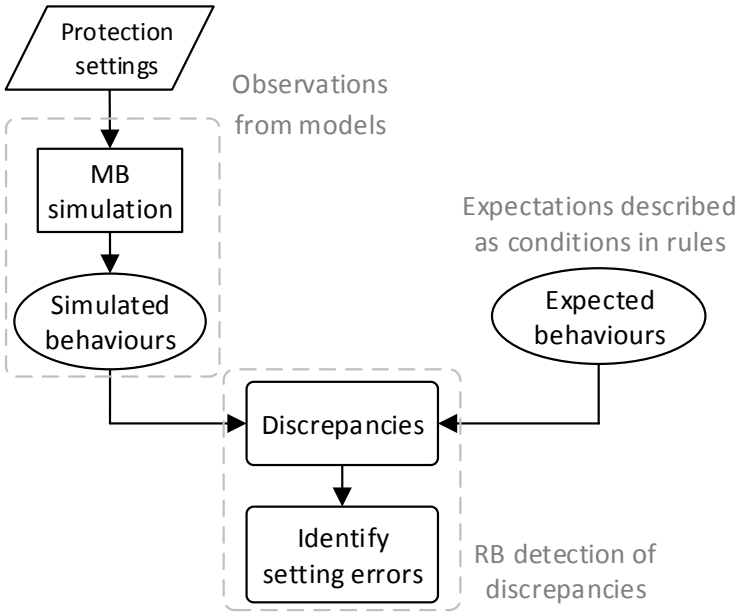


Figure 5.12: MB validation of protection settings

of problems in settings or in the design of the protection system, which is clearly important and advantageous to know in advance of actual commissioning and deployment of the protection scheme. The automatic detection of discrepancies is performed by the RB module, where the information regarding the incorrect operating elements and the nature of the detected problems is also provided.

In this section, the design of an MB module that performs the aforementioned validation task is presented in detail. Specifically, the MB module automatically populates equivalent network models, configures IED models using the settings to be validated, creates a set of credible system events that cover a very wide range of operational scenarios that could be encountered, and simulates the protection IEDs' behaviour in response to these events. The automated process is achieved by an interface layer within the MB module that allows interaction with a commercially available PowerFactory simulation engine to leverage its internal data and functions to be used for the tasks of protection settings and performance validation. As noted previously, the simulation results are inserted into the RB module and analysed automatically, thus allowing the entire MB validation process to be automated, which can not be achieved in any existing commercial systems for the settings validation task.

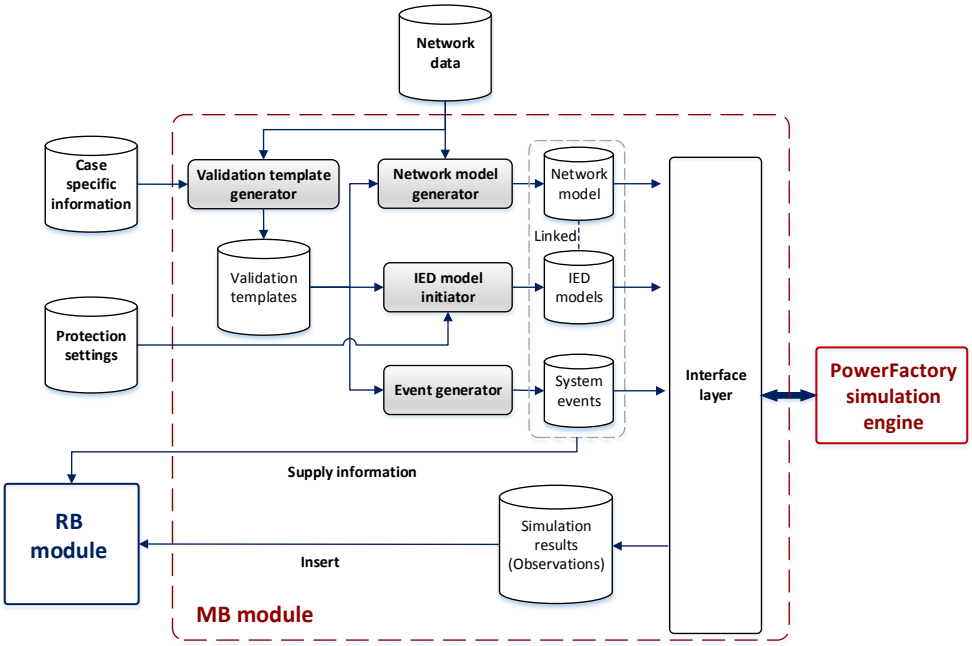


Figure 5.13: Schematic of the MB module architecture

5.4.1 The Structure of the MB Module

The overall architecture of the MB module is shown in Figure 5.13. The module contains the following main components: validation template generator, network model generator, IED model initiator, event generator, and interface layer.

The inputs to the MB module are the network data (imported automatically by the data importer from a number of CSV-based network data files), the protection settings data (imported and interpreted by parsers in the data importer), and case-specific information (e.g. the protection scheme being validated supplied by the user). The outputs are the simulation results (observations) that are inserted to the RB module for automated analysis, where a summary of assessment of all simulated operations is provided. The simulation results can also be reviewed if needed to facilitate the interpretation of the automated analysis results from the RB module.

The process of using the MB module for the settings validation is illustrated in Figure 5.14. The functional allocation of the main components and the key steps during the validation process can be summarised as follows:

1. The validation template generator selects a validation schedule (a pre-

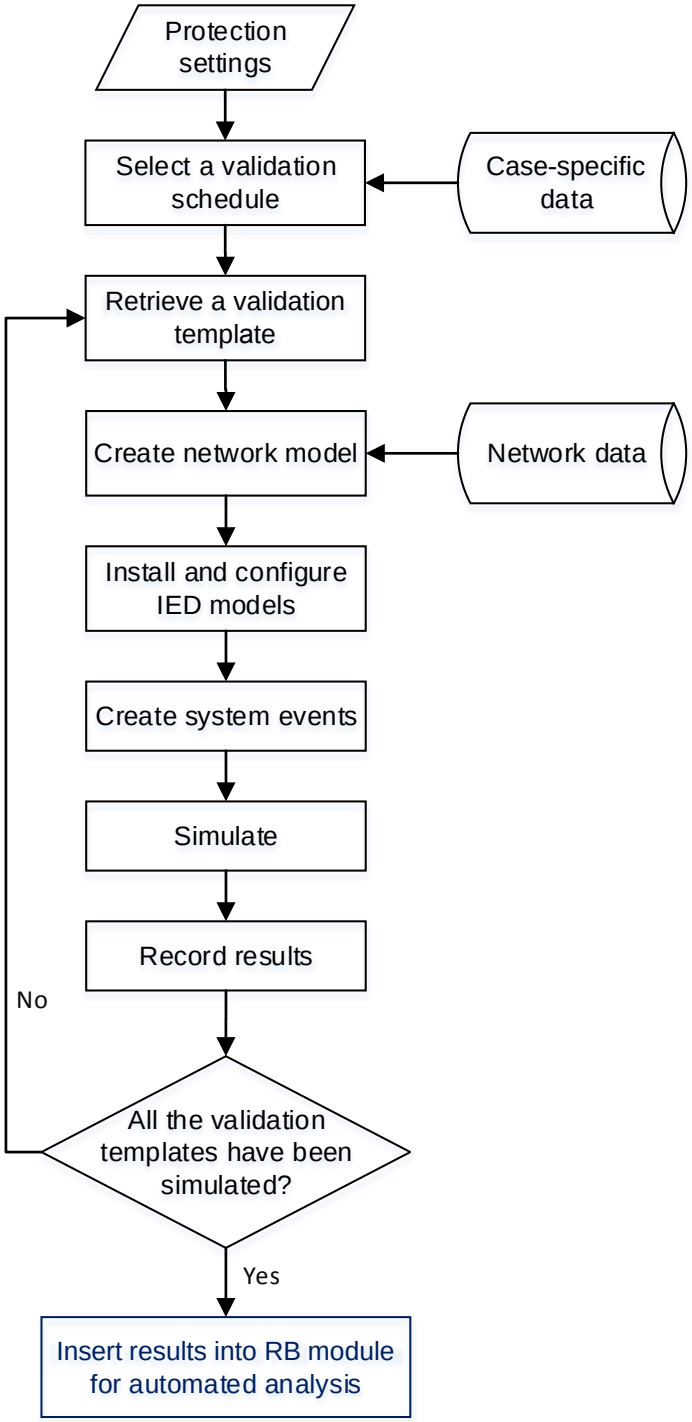


Figure 5.14: The process of MB protection settings validation

defined schedule for testing a specific protection scheme - further details are provided in Section 5.4.2) based on the supplied case-specific information. Within each validation schedule, there may be a number of validation templates defined for testing various aspects of the protection scheme, e.g. sensitivity and stability of feeder differential protection scheme.

2. From the available validation templates of a validation schedule, one validation template is retrieved, which specifies the network models to be used and the system events to be simulated.

3. The retrieved validation template is used by the network model generator to populate network models for simulation.

4. The IED models are installed in the created network model by the IED model initiator, and configured using the settings to be validated.

5. A set of system events are automatically generated by the event generator based on the information presented in the validation template.

6. The system events are simulated and the results are stored.

7. Start with another validation template until all the templates have been simulated.

8. The observations from the simulation are inserted to the RB module for automated analysis.

5.4.2 Validation Template Generator

The MB validation process is performed according to pre-defined validation schedules, and each validation schedule contains a number of validation templates for testing a specific protection scheme. The validation template generator is responsible for selecting an appropriate validation schedule for the protection scheme being validated and retrieving the associated validation templates for simulation.

For example, FM_DIFF (i.e. first main differential protection) is a validation schedule defined for the feeder differential protection scheme. In FM_DIFF, there

are two default validation templates for testing the stability and sensitivity of the scheme, which are described in Table 5.3. DIFF_STAB is provided to test whether the settings can provide sufficient stability under maximum external fault conditions (with fault curents up to the switchgear rating). A network model, termed "simplified" is used, which is a type of equivalent model that only contains the protected equipment and its connected nodes. More discussions on the equivalent model types defined in this work are provided in Section 5.4.3. The maximum fault infeeds are supplied from the connected nodes and bolted Ph-E and Ph-Ph-Ph faults are applied on both nodes to test whether the IEDs would remain stable. The template DIFF_SENS aims at testing whether the settings are sensitive enough for detecting minimum fault conditions, which are defined by the scenarios where only single-end infeed is available and Ph-E and Ph-Ph-Ph faults with 100 Ω resistance occur at the remote end of the feeder. In this template, two simplified models are populated with single-end infeed from either end, and faults are applied at the end of the feeder (i.e. the opposite to the end with fault infeed) to test whether the IEDs would operate to isolate these faults. In Chapter 6, an example is provided to demonstrate this process in action.

The two validation templates (DIFF_STAB and DIFF_SENS) within the validation schedule FM_DIFF are default validation arrangements and represent two "worst-case" scenarios in terms of testing the performance of a protection system at its limits, i.e. maximum fault-infeed external faults and minimum-infeed highly-resistive internal faults (the maximum and minimum fault infeeds and line data are derived from circuit data supplied by National Grid). Additional templates can be manually defined, which may use more detailed network models for testing internal and external faults with various impedances. Further work could investigate future performance - e.g. under progressively weaker infeeds, with converter-interfaced sources (which may delay supply of fault current from one end) - using different validation templates.

Name	Network model	Fault event
DIFF_STAB	Simplified model: maximum fault infeed (switchgear rating)	Ph-E and Ph-Ph-Ph faults at connected nodes, 0 Ω
DIFF_SENS	Simplified model: single-end minimum fault infeed	Ph-E and Ph-Ph-Ph faults at remote end of the feeder, 100 Ω

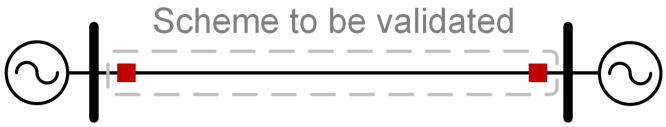
Table 5.3: Validation templates for feeder differential protection

5.4.3 Network Model Generator

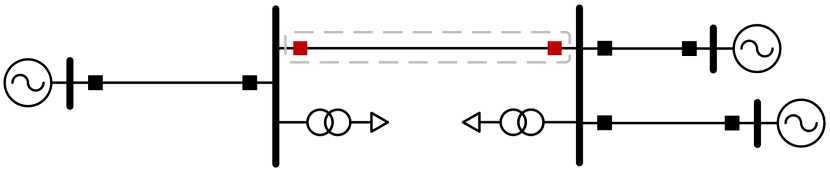
The network model generator is responsible for populating appropriate network models as specified in the validation templates for the MB simulation. In this work, three default model types are defined for validating various feeder protection schemes, i.e. simplified, standard and advanced network model. As shown in Figure 5.15, these equivalent network models include different levels of details of the network, which can be used to suit the need for testing different protection schemes. The equivalent infeed source impedance for each model type can be further configured for different validation purposes. For example, in the feeder differential protection as discussed in the previous section, the simplified model type is used to test and validate both stability and sensitivity, with the source impedance configured to simulate maximum and minimum fault infeed conditions.

5.4.3.1 Default Equivalent Network Models

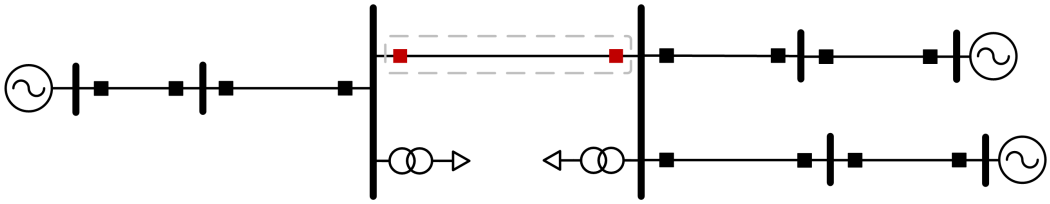
The simplified network model, as shown in Figure 5.15a, contains only the protected equipment and the nodes it is connected to. For three-ended networks, three nodes are included in the model. Although the model is very basic, it is sufficient to be used for certain validation functions such as the validation templates for feeder differential protection as discussed previously. In the developed system, it is also used for simulating the protection operation of feeder overcurrent protection and earth fault protection, where the operating time for faults at the local and remote ends are the main concerns.



(a) Simplified equivalent network model



(b) Standard equivalent network model



(c) Advanced equivalent network model

Figure 5.15: Network models used for MB validation of protection settings

The standard model, as shown in Figure 5.15b, includes the protected equipment and the adjacent circuits that are connected the nodes of the protected equipment. There is also a transformer model installed at each end of the feeder to represent the parallel-connected transformers at the two ends. In the developed system, this model has been used for the validation of distance protection schemes, where faults can be applied in the forward and reverse directions from the perspective of the relay's measurement point for testing various zone reaches. In practice, it is possible that the zone 3 reaches of distance protection may reach beyond any immediately-adjacent feeders in the forward direction. It is normally still acceptable to use the standard model for validation of zone 3 reaches, as the main concern with zone 3 reaches is ensuring that they do not encroach onto the lower voltage network (i.e. reach "through" a transformer) and that they cover at least all adjacent circuits connected to the remote end. This check can be achieved using this standard model. If more detailed investigations of zone 3 reaches are required, the advanced model, as described below, can be used.

The advanced model is shown in Figure 5.15c and is provided for the validation

Template	Fault Type	Fault location
Dist_Pro_1ph	Ph-E	1%, protected feeder
Dist_F1_1ph	Ph-E	1%, F1 branches

Table 5.4: Example templates and associated fault events for MB validation of feeder distance protection

of distance protection when a more detailed investigation (particularly zone 3 reaches) is required. The main difference of the advanced model from the standard model is that equipment within three levels of depth (i.e. including primary, secondary and tertiary branches) in the both forward and reverse direction are included in this type of model.

Appendix A presents details relating to how these models are using the provided circuit data.

5.4.4 Event Generator

The event generator creates system events (e.g. faults) based on the validation templates and the associated network models used. The generated fault events contain the information about the faulted equipment, fault location, fault types, and fault impedance. Table 5.4 shows two of validation templates defined for feeder distance protection scheme and their fault events created. In Dist_Pro_1ph, standard network model is used, and Ph-E faults with zero impedance at all locations along the main protected feeder (at steps of 1% along the entire feeder) are applied, while in Dist_F1_1ph, the standard network model is used, but faults are applied on all of the adjacent feeders connected to the remote end of the main protected feeder (referred as F1 branches). The use of the event generator allows the creation of a large number of faults events automatically.

5.4.5 Interface with DIgSILENT PowerFactory Simulation Engine

The validation template generator, network model generator, IED model initiator and event generator prepare all information required for simulation. The actual simulation process is performed with the aid of an external simulation engine using an interface layer to leverage the engine's internal data and functions to perform the defined simulation processes as a batch process. In the developed system, the commercially-available PowerFactory simulation engine has been adopted, because:

- It includes comprehensive validated IED models for most of the existing commercially-available protective devices and the library of devices is periodically upgraded.
- It provides the interface that allows the manipulation of its simulation functions and data by external applications. This is achieved through the provided application program interface (API) (discussed in more detail later). Similar approaches that use existing models and simulation engines from external applications are reported in [MBL+98, DMM03].
- Practically, PowerFactory is widely used by GB transmission network operators to model their networks. The use of PowerFactory aligns well with the available network data.

In practice, the use of the PowerFactory simulation engine is not a unique or mandatory option. Any system that offers appropriate MB simulation engine and models, and provides access to their functions for external applications can be considered as candidates for this purpose. The methodology and design approach presented in this thesis could be implemented using a different set of simulation engines and input data sources, with appropriate interfaces.

The PowerFactory API provides a library of functions that allows access to internal data and functions from external applications. This is implemented as a

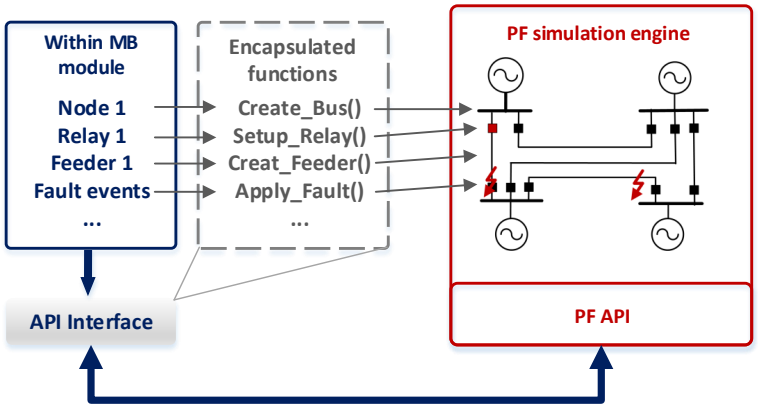


Figure 5.16: The interface between MB module and PowerFactory simulation engine

list of Dynamic Link Libraries (DLL) files [DIg11b]. The internal PowerFactory functions are basic and generic, e.g. there is no readily-available function for creating and configuring a relay model. The role of the interface layer is to encapsulate these basic and generic functions and packages them into new functions that are tailored for the settings validation task, and use the tailored functions to perform and properly-configured credible simulations for the purposes of protection settings validation based on the information supplied by other elements within the MB module (e.g. the network generator and validation template generator). Figure 5.16 shows a number of example functions that illustrate how the interface layer interacts with the PowerFactory simulation engine for tasks such as constructing network model, configuring IED models and applying faults.

A practical issue associated with interfacing MB module with the PowerFactory API is the different programming languages used to implement the different modules (MB module in Java and PowerFactory API in C++). This issue can be addressed using tools such as SWIG [SWI15] which allows connections to be made between software applications or modules created using C++ and other modules implemented using a range of other high-level programming languages.

5.4.6 RB Interpretation of MB Results

The results data from the MB simulation has the potential to be overwhelming if manually interpreted. This is due to the large number of protective devices

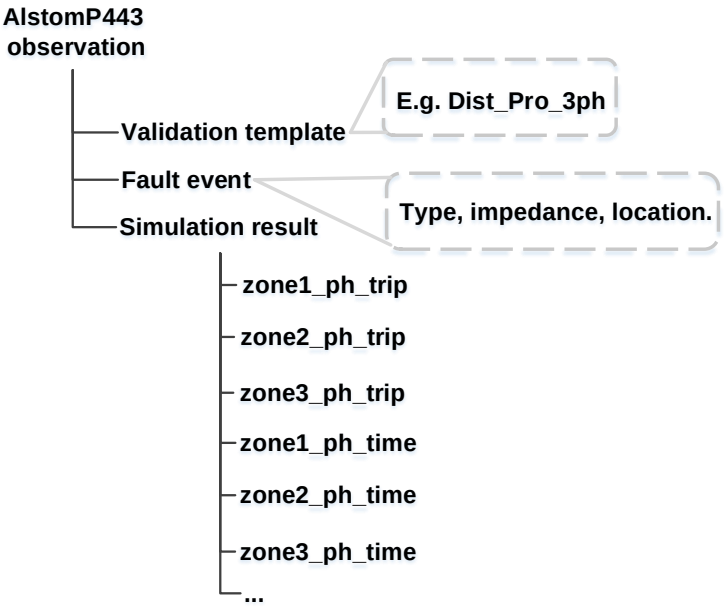


Figure 5.17: An example observation from MB simulation

available in the network, each of which may need to be simulated using various validation templates and associated defined events. Therefore, the RB module is used for the automatic analysis of the simulation results so that any undesired operations can be detected and reported without the need for manual input, and any erroneous behaviour can be filtered from the other large volumes of information and brought to the attention of the user.

To develop rules for detection of incorrect operations during simulation, the expected IEDs' behaviours (i.e. expectations) under certain validation templates and fault events need to be defined. In the rules' conditions, inverse logic is applied, i.e. the conditions specify the undesired operation of an protection element under certain simulated event within a certain validation template, if the conditions are fulfilled, which would fire the associated rules, it is considered that incorrect operations have been detected.

Figure 5.17 shows an example of how an observation from the simulated event is defined, where it can be seen that the observation contains information relating to simulation results for each protective element in the protection IED (e.g. the tripping status of a distance protection zone) and the validation template and fault event under which the protection operations are observed.

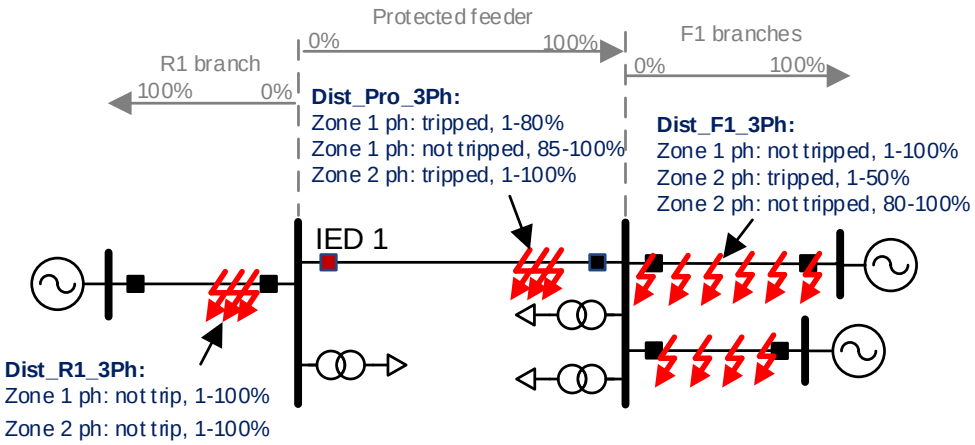


Figure 5.18: Example expectations of a distance protection scheme in a circuit diagram view

Figure 5.18 shows a number of examples of expected behaviours of the phase distance zones Zone 1 Ph and Zone 2 Ph in IED 1 with respect to various validation templates and fault events. For testing the distance protection scheme, all validation templates have used the same network model (as shown in Figure 5.18). Dist_Pro_3ph, Dist_F1_3ph and Dist_R1_3ph are validation templates for testing IED 1's operation when Ph-Ph-Ph faults are applied in the protected feeder, forward remote connected branches (i.e. F1 branches as shown in Figure 5.18) and reverse branches (i.e. R1 branches as shown in Figure 5.18) respectively. Full descriptions of these validation templates for the feeder distance protection scheme are provided in Chapter 6, where a case study that uses such validation templates for MB validation is also provided.

Taking the template Dist_Pro_3ph as an example, Ph-Ph-Ph faults with zero impedance are applied across the protected feeder, where it is expected that Zone 1 Ph should trip for faults that are situated at locations that are less than 80% of the line length away from IED 1, while it should remain stable for faults beyond 85% of the line. Here a tolerance of 5% is applied where operation or non-operation in the reach points between 80-85% are both considered to be acceptable. For the same template, Zone 2 Ph should trip for all fault applied in the protected feeder. Table 5.5 lists the rules for detection of undesired operations against exceptions in the template Dist_Pro_3ph for Zone 1 Ph. In this case, since all faults applied in Dist_Pro_3ph are Ph-Ph-Ph faults with zero impedance,

	When	Then
1	Template used is Dist_Pro_3ph; fault location < 80%; zone1_Ph_trip is false	**Error**: Zone 1 Ph has not provided a sufficient reach.
2	Template used is Dist_Pro_3ph; fault location > 85%; zone1_Ph_trip is true	**Error**: Zone 1 Ph has over reached for faults beyond 85% of the protected line.

Table 5.5: Example rules for identifying incorrect operations of Zone 1 ph

such information is not included in the conditions of the rules. The execution ("then") part of the rule lists the messages generated when incorrect operations are detected.

5.5 Conclusions

This chapter has presented the hybrid RB and MB approach for validation of protection settings and subsequent protection scheme performance through the description of the design and operation of the intelligent system PPST. The RB module checks the settings against the rules translated from setting policies, while the MB module is provided for a further means of validation of protection performance during operation by simulating the behaviours of protection schemes under various system events. The provision of the MB module also allows the potential weaknesses of the setting policies to be detected, so that improvement on the policies can be conducted when such scenarios are identified.

The entire validation process (using both RB and MB modules) is automated with minimum manual input. Specifically, the MB module automatically populates network models, configures IED models, creates and simulates system events, and analyses simulation results, which cannot be achieved in any existing MB systems for the validation of settings. The automated simulation process is achieved by the provision of an interface layer that allows interaction with the PowerFactory simulation engine. The analysis of simulation results is automated

by the application of pre-defined rules to interrogate whether the simulated observations are consistent with the defined expectations. The high level of automation during the validation process allows a large number of setting files to be validated with minimal manual input, which is particularly beneficial given the significant number of protective devices and their associated setting parameters available in the system.

Chapter 6

Case Studies

6.1 Introduction

As a demonstration of the methodology and design approaches presented in Chapter 5 for the validation of protection settings, a prototype intelligent system PPST has been implemented. In this chapter, case studies relating to the application of PPST for validating settings from feeder differential and distance protection are presented. These two protection functions have been selected for demonstration because they are invariably used as the two main protection schemes for feeder protection in the GB transmission network, and the validation of these functions represents a major part of the task for validating the settings in the entire network.

Section 6.2 provides an overview of the developed PPST prototype. In Section 6.3, a case study concerned with the validation of feeder differential protection is provided, where manual errors have been introduced when entering the settings data to the IEDs, and such errors are successfully detected by the RB module, which allows the settings to be amended. The updated settings are re-validated by the RB module with no error detected, and the results are verified in the subsequent performance which is analysed by the simulation-based validation process in the MB module. In Section 6.4, the use of PPST for validating feeder distance protection scheme is demonstrated, where settings based on obsolete

setting policies are detected and considered erroneous by the RB module that is equipped with rules translated from the most-updated policies. In the subsequent MB stage, an additional error (reflective of an actual historical incident) that is overlooked by the RB module is detected in the performance analysis through simulation. Further investigations of protection performance using the MB module have been conducted, where additional problems that not detected by the RB module are identified.

6.2 The PPST Prototype

The current version of PPST has the following main components and features:

- A data importer that is capable of automatically importing all of the network data that is relevant to protection functions (including data from feeders, transformers, and fault levels at each busbar) from CSV-based files and storing it in the internal relational database.

- A number of parsers that allow the interpretation of settings data from files in the formats of XRIO and CSV. The supported IED types include [Sie11b, Sie00, Als11b, Als11a, ABB12, ABB14, GE 12a, GE 12b].

- A user-friendly GUI element that facilitates interaction between users and the system. A graphical analysis tool is also provided for assisting the settings validation task and to present various means of graphical analysis of protection characteristics.

- An RB module that is capable of performing the validation of all feeder protection schemes (i.e. differential, distance, phase overcurrent and earth fault protection) using rules translated from a GB transmission network operator's setting policies. The RB module also contains rules for automatic analysis of the MB simulation results to identify incorrect operations. The current version of the tool allows the identification of the exact incorrect operation units in the IEDs (e.g. a distance protection zone).

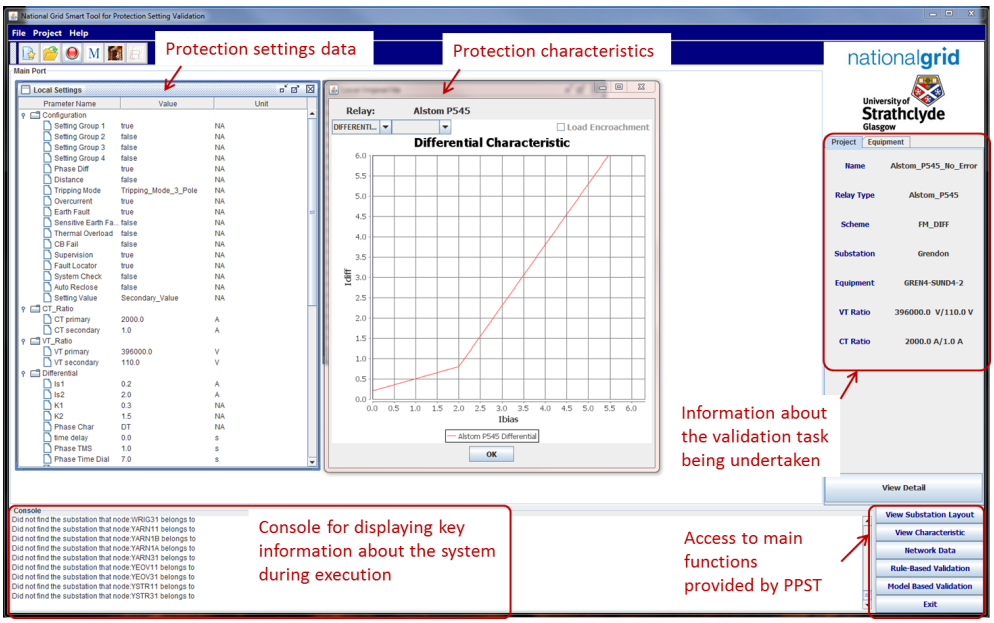


Figure 6.1: The main GUI of PPST with differential protection settings data imported

- An MB module that is capable of automatically performing validation of all feeder protection schemes. The current version considers feeders and transformers in the equivalent network model, and the system events used for testing are faults with various types, impedance and locations.

Figure 6.1 shows the main user interface of PPST, where a project has been created, and the imported settings data and the protection characteristics (the differential protection biased characteristic in this case) are shown. The imported settings are presented in a tree view, which is reflective of the way that they are structured in the original IED. The displayed protection characteristics are constructed using the imported settings data. The console displays key information during the system execution, e.g. presenting any important messages relating to any abnormal issues arising during the import of circuit and protection settings data. A brief summary of the validation task being undertaken is provided in the panel on the right hand side, which includes information relating to the IEDs being used and protection scheme being validated. A panel containing multiple buttons is provided at the bottom-right corner of the display which allows the users to access the main functions provided by PPST, e.g. RB and MB validation of settings, graphical analysis of protection characteristics, access to the entire

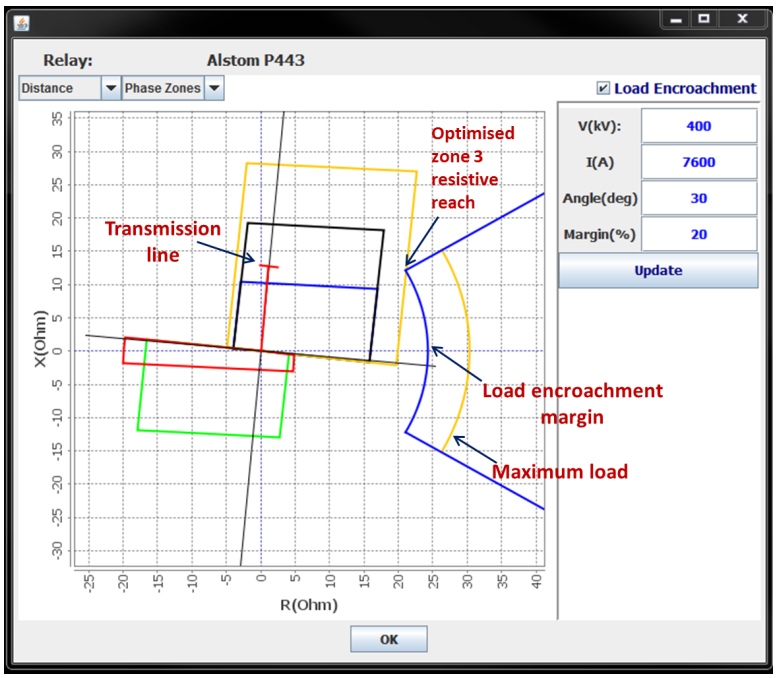


Figure 6.2: Graphical analysis tool to assist protection settings validation

network's circuit data, ability to display views of substations' layouts and running arrangements, etc.

Figure 6.2 shows an example of the use of the graphical analysis tool within the GUI element to facilitate the validation and analysis of distance protection settings. In this example, the maximum load and the load encroachment margin defined by the policies are plotted. The zone reaches in relation to the transmission line impedance can be viewed in an intuitive manner. The load encroachment margin is the boundary that the reach of the protection zones should not exceed in order to avoid mal-operation during heavy loading conditions. In this case, the zone 3 resistive reach has been optimised, i.e. to offer maximum resistive fault coverage while avoiding encroachment on the defined marginal area. Such graphical functions, although not critical to the work reported in this thesis or the core functionality of the error detection functions, provide an useful and intuitive method to assist users in analysing the validity of protection settings. As already mentioned on a number of occasions, the RB and MB modules are the main elements responsible for the validation task, and they are demonstrated using examples in the next two sections.

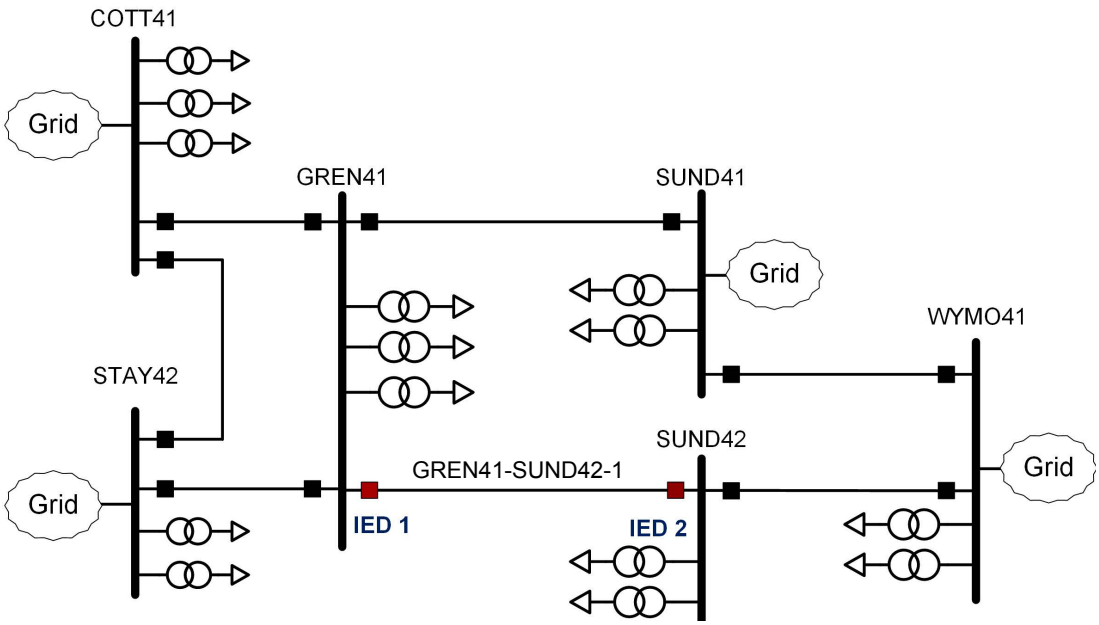


Figure 6.3: The circuit and the IEDs involved in the case studies

6.3 Case Study 1: Validation of Protection Settings for Feeder Differential Protection

In this case study, a feeder differential protection scheme is validated, where commercially available IEDs [Als11a] are used. The circuit being investigated is GREN41-SUND42-1 within National Grid's network, and the protection scheme involves the use of IED 1 and IED 2 installed in the node GREN41 and SUND42 respectively as shown in Figure 6.3, with the associated equipment data provided in Appendix B.1.

6.3.1 RB Validation

Each of the IEDs in use contains more than 100 setting parameters, among which 95 settings that are most relevant to the protection scheme have been considered in the PPST prototype (other available settings can be relevant to functions such as communications). To validate such a scheme, 89 rules have been implemented. The number of rules is smaller than the settings, because one rule may be relevant to multiple settings. For example, when checking the sensitivity of the protection

Setting	Description	Available settings
Phase Diff	To enable or disable the differential protection function.	Enabled or Disabled
Auto-Reclose	To enable or disable the Auto-Reclose function.	Enabled or Disabled
I_{s1}	Minimum pick-up current level of the relay.	Numeric
I_{s2}	The bias current threshold, above which the higher percentage bias k_2 is used.	Numeric
k_1	The lower percentage bias setting used when the bias current is below I_{s1}.	Numeric
k_2	The higher percentage bias setting used to improve relay stability under heavy through fault current conditions.	Numeric

Table 6.1: The description of the settings being investigated in case study 1 [Als11a]

scheme as presented later in this section, two settings that govern the biased characteristic of the differential protection have to be checked in one rule.

In this study, a subset of settings that contain different types of errors have been selected for demonstration. The selected settings are listed and described in Table 6.1. The values of the settings of the two IEDs are presented in Table 6.2, with IED 1's original settings containing a number of deliberately-introduced errors and new settings are amended based on the RB validation results as discussed later.

The settings are validated in the RB module, and the associated validation rules are provided in Appendix B.2.1. Figure 6.4 shows the user interface that displays the validation results of IED 1's settings. The validation results are presented in a tree view with the aid of colour coded indicators, where errors are represented in red, warnings in yellow, and correct settings in green. The grey indicator represents the settings that are not validated by any rules, i.e. there is

Setting	**IED 1 (original)**	**IED 1 (new)**	**IED 2**
CT primary	2000 A	2000 A	2000 A
CT secondary	1 A	1 A	1 A
Phase Diff	Enabled	Enabled	Enabled
Auto-Reclose	Enabled	Disabled	Disabled
I_{s1}	0.2	0.2	0.2
I_{s2}	2.0	2.0	2.0
k_1	0.5	0.3	0.3
k_2	1.3	1.5	1.5

Table 6.2: The values of the settings being investigated in case study 1

no associated applicable rule(s) specified within the policies. These settings are those that are not directly allocated to any protection functions. For example, in this case, VT ratio primary and secondary settings and the setting parameter to control the primary or secondary value to be used for configuring numeric settings in the IED are not validated by the RB module. While they are not checked, the grey indication is useful, as it alerts the user to this fact and therefore the user can manually pay more attention to the validity of these specific settings.

In the illustrated example, the parameter "Auto-Reclose", "k_1" and "k_2" in IED 1 are considered to be erroneous. The function block, "Differential", is also marked as erroneous because there are detected errors in its children "k_1" and "k_2". Such an approach is provided for easy location of identified errors. On the right-hand side, a summary of the validation results is presented, which provides information on the number of total settings, errors, warnings, etc. In this case, it shows that 95 settings have be evaluated; 3 of the settings are considered to be erroneous; 3 settings have not been validated; and no warnings have been raised.

For each detected error, more detailed information is also provided to specify the currently-configured value, suggestions for improvement, and the rule(s) that the setting violates. One example for a detected error in "k_2" is shown in Figure 6.5, where it shows that the error is a consequence of the two settings ("k_1"

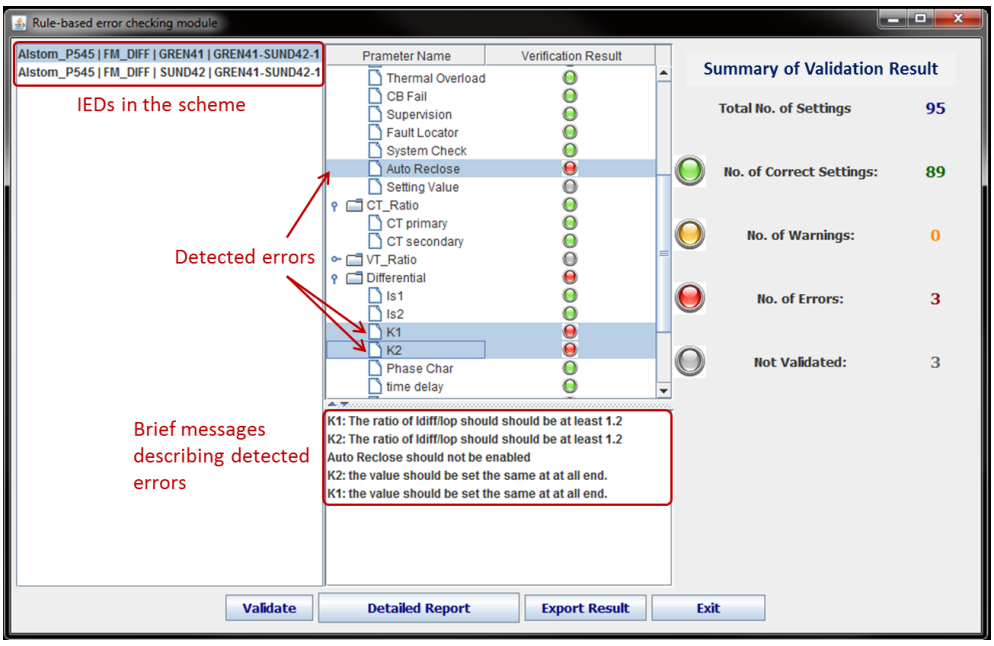


Figure 6.4: The RB validation results for IED 1

and "k_2"), which fail to provide sufficient sensitivity under the minimum fault condition (the definition of such a condition and more details on the reasoning are available in Appendix B.2.1). In this case, since there are two variables determining the sensitivity of the scheme, no specific suggested value for each setting is provided. However, a message is generated to specify the condition that "k_1" and "k_2" must fulfil during the minimum fault condition to provide sufficient sensitivity, i.e.

$$I_{op} = I_{s1} + k_1 \times I_{s2} + k_2 \times (I_{bias} - I_{s2}) <= 0.886A$$

where I_{op} and I_{bias} are the current required for the protection to operate and the bias current under minimum fault condition. More details on how these quantities are defined, and the associated calculations performed by the rules, are available in Appendix B.2.1 and Appendix B.3.3 respectively. Where possible, PPST has been designed to provide suggested values for the erroneous settings that would comply with the setting policies. A number of such examples are provided in Section 6.4.

Table 6.3 and Table 6.4 present all of the detected errors and the associated

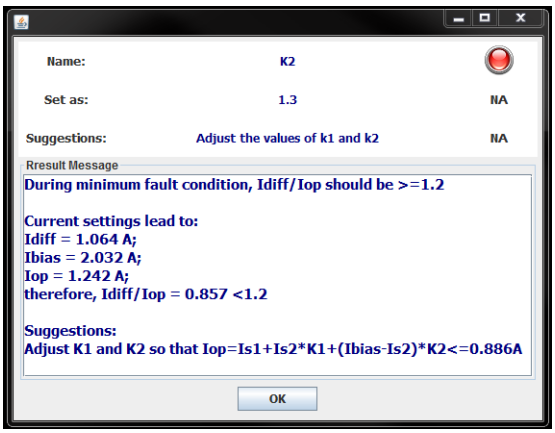


Figure 6.5: Detailed information on the identified error in k_2

details generated from the validation results for IED 1 and IED 2 respectively. In IED 1, "Auto-Reclose" is inadvertently enabled (detected by the functional configuration rules); "k_1" and "k_2" are assigned with values that do not offer sufficient sensitivity during minimum fault condition (detected by the calculation validation rules); and both "k_1" and "k_2" are set different from the remote end IED's values (detected by the coordination rules), which is not permissible, and similar errors have therefore been detected for IED 2 as shown in Table 6.4.

A summary of all validation results and the associated suggestions can be exported in a text-based file. Figure 6.6 shows the validation summary for IED 1, where all of the information contained in Table 6.3 is represented in a text file for documentation purpose.

Based on the information provided in the validation results, the settings of IED 1 are amended to be the same as IED 2's settings as shown in Table 6.2. The settings are then re-validated in the RB module and the results show the amended settings conform with all rules. The new settings are then inserted to the MB module for further validation.

Result	Setting	Detailed message
Error	Auto-Reclose	Should be disabled for feeder differential protection.
Error	k_1	During minimum fault condition, I_{diff}/I_{op} should be ≥ 1.2. Current setting leads to : I_{diff}= 1.064 A, I_{op} = 1.242 A, I_{diff}/I_{op} =0.857. Suggestion: Adjust k_1 and k_1 so that I_{op} <=0.886 A.
Error	k_1	k_1 should be set the same at all ends. Local: 0.5. Remote: 0.3.
Error	k_2	During minimum fault condition, I_{diff}/I_{op} should be ≥ 1.2. Current setting leads to : I_{diff}= 1.064 A, I_{op} = 1.242 A, I_{diff}/I_{op} =0.857. Suggestion: Adjust k_1 and k_1 so that I_{op} <=0.886 A.
Error	k_2	k_2 should be set the same at all ends. Local: 1.3. Remote: 1.5.

Table 6.3: The detected setting errors in IED 1

Result	Setting	Detailed message
Error	k_1	k_1 should be set the same at all ends. Local: 0.3. Remote: 0.5.
Error	k_2	k_2 should be set the same at all ends. Local: 1.5. Remote: 1.3.

Table 6.4: The detected setting errors in IED 2

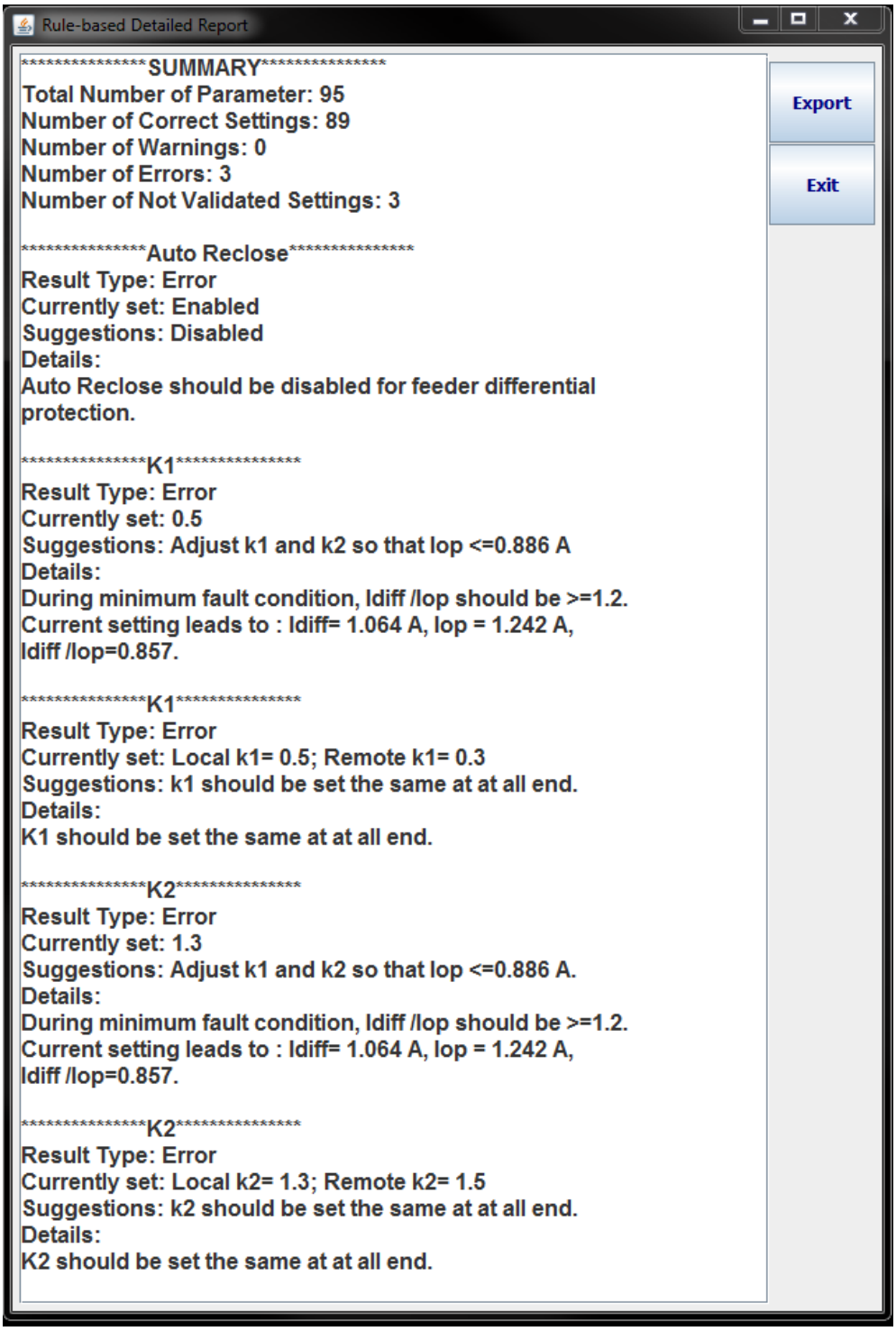


Figure 6.6: A text-based file containing the summary of validation results of IED 1

6.3.2 MB Validation

In the MB module, there are two validation templates defined for the feeder differential protection scheme, i.e. DIFF_SENS and DIFF_STAB.

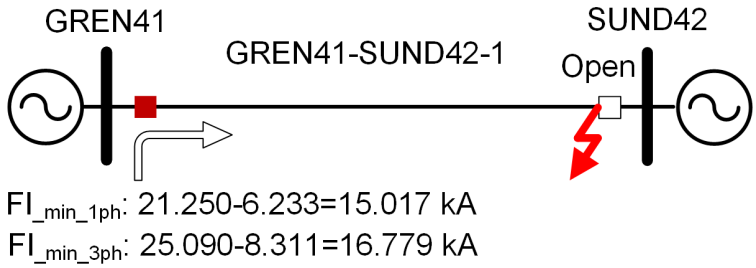
The template DIFF_SENS is provided for checking of the sensitivity offered by the configured settings, where two equivalent network models shown in Figure 6.7 are populated. FI_{min_1ph} and FI_{min_3ph} are the minimum single-phase and three-phase fault infeeds, and the detailed fault level data is available in Appendix B.1. In Figure 6.7a, the model (referred to as GREN41_min_infeed) represents the situation where there is minimum fault infeed from the node GREN41 with the circuit breaker at SUND42 end open, and Ph-E and Ph-Ph-Ph faults with 100 Ω resistance are applied at the remote end (i.e. SUND42) of the feeder, to test whether IED 1 is capable of detecting such faults. The model (referred as SUND42_min_infeed) in Figure 6.7b is populated for the same purpose but for testing IED 2's settings. These two scenarios are considered to be the worst-case operating conditions, where if the settings enable the IED to be capable of detecting the faults, then it is considered that the settings offer sufficient sensitivity for all other scenarios.

For the validation of stability, the template DIFF_STAB is used, where maximum fault condition with single-phase (FI_{max_1ph}) and three-phase (FI_{max_3ph}) fault infeed currents up to switchgear rating (i.e. 63 kA) are considered. The model shown in Figure 6.8 is populated for the test. Ph-E and Ph-Ph-Ph faults with zero impedance are applied at both nodes to test if IED 1 and IED 2 will remain stable. If they do, then it is considered that sufficient stability has been provided. The details of the equivalent source impedance in all populated models are provided in Table 6.5. These templates are simulated in the MB module and the simulated operations are analysed using the rules presented in Appendix B.4.1 to automatically identify incorrect operations.

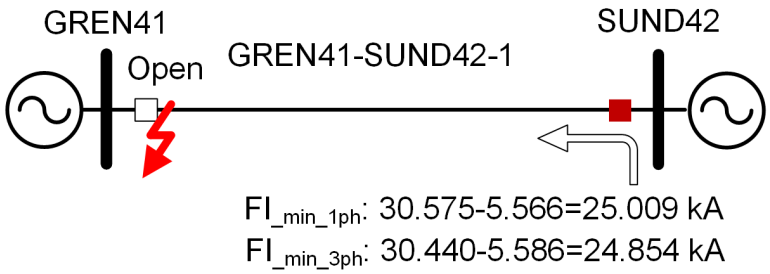
A summary of the outcomes from analysing the simulated protection behaviours is shown in Figure 6.9. The table in the centre of the user interface provides details on all the simulated validation templates and the associated

Network model	**Node**	Z_{eq1}, Z_{eq2} (Ω)	Z_{eq0} (Ω)
GREN41_min_infeed model (Figure 6.7a)	GREN41	13.764	18.608
	SUND42	-	-
SUND42_min_infeed model (Figure 6.7b)	GREN41	-	-
	SUND42	9.292	9.119
DIFF_STAB model (Figure 6.8)	GREN41	3.666	3.666
	SUND42	3.666	3.666

Table 6.5: The source equivalent impedance for the constructed network models



(a) GREN41_min_infeed model



(b) SUND42_min_infeed model

Figure 6.7: Network models populated for DIFF_SENS

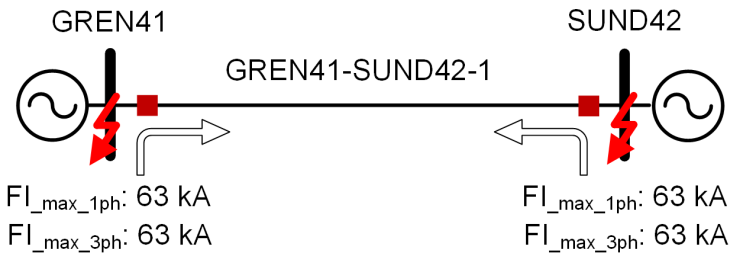


Figure 6.8: Network model populated in template DIFF_STAB

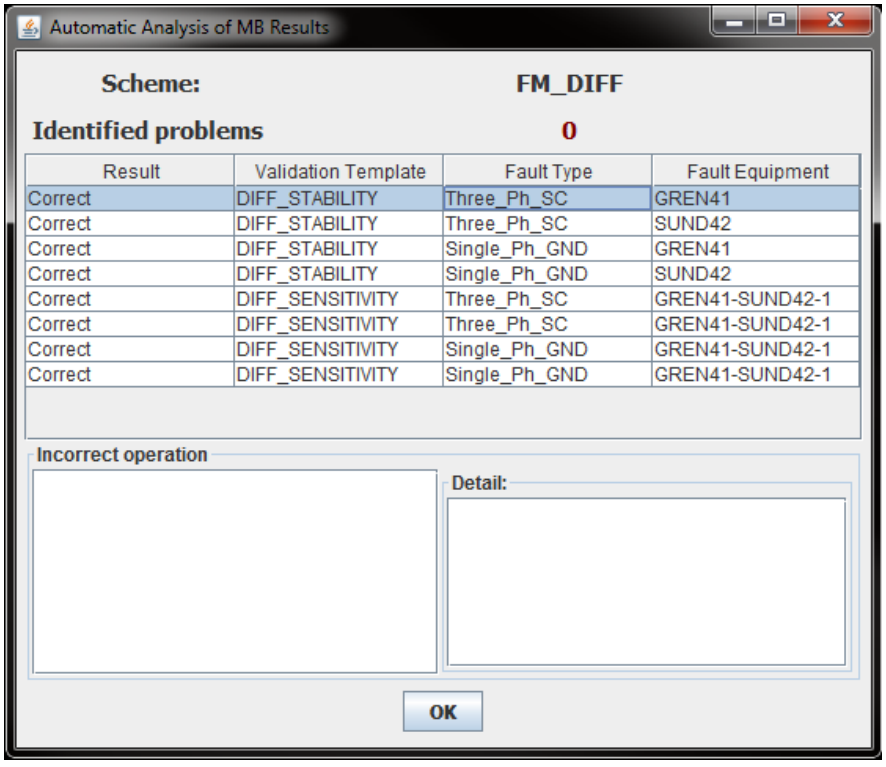


Figure 6.9: MB validation result when there is no setting error

fault events, along with the assessment results of operations (i.e. correct or erroneous). If there are incorrect operations detected, they will be listed separately in the bottom-left panel, with detailed information on the undesired operation provided in the bottom-right panel. In this case, the settings have resulted in correct operations in all of the simulations defined in the validation templates, which verifies the RB validation results. Therefore, the two panels on the user interface, designed for showing incorrect operations, are empty in this case. In the following case study, scenarios where the MB module detects incorrect operations that were not identified in the RB module are provided.

6.4 Case Study 2: Validation of Protection Settings for Feeder Distance Protection

Setting policies are reviewed regularly and updated when necessary to ensure the specified requirements for settings can provide optimised solutions for the protection systems. When the policies have been updated, a key challenge is to ensure that all settings in the network conform to the most updated version of the policies. Currently, there is no routine provision in the GB transmission network for comprehensive validation of protection settings after the update of the policies, due to the numerous setting files and the associated setting parameters available. There are cases where the settings considered correct in previous version(s) of policies may no longer be fit for purpose for the prevailing system conditions, and therefore considered erroneous by the current policies. In this case study, the use of PPST to detect such scenarios is demonstrated.

In some circumstances, only relying on the rules translated from policies may not be sufficient. In this case study, a particular scenario that is overlooked by the RB module and is reflective of an actual mal-operation event in the GB transmission system has been selected to demonstrate how the MB module can detect incorrect protection operations to identify potential setting errors. On 28 August 2003, a protection mal-operation event led to the loss of supply in south London, and the investigation showed that one of the main causes of the event was the in-

correct selection of the backup IDMT relay's rating, i.e. a relay that mismatched to the actual CT secondary nominal current was used [Nat03]. Although such an error was caused by a mistake in the selection of the physical devices, which is out of the scope of this work, similar errors may arise when setting the CT and VT parameters in modern IEDs and could lead to a subsequent failure in the protection system. In this case study, a scenario based on this incident has been developed. It is shown that, solely relying on the rules translated from the policies may result in failure to detect such errors (although they are simple), and the provision of the MB module as a further means of checking would allow such problems to be detected so that they can be included in the RB module for future validation.

Figure 6.10 shows an overview of the case study, where a distance protection scheme is validated using PPST. IED 1 is selected as the protective device to validate for demonstration. It originally contains four setting errors in its setting file. Three of the settings (i.e. "R3 Ph Res Fwd", "R3 Ph Res Fwd" and "IN3 Current Set", which are described in Table 6.6) are based on old setting policies and are now deemed to be incorrect by current policies, and they are successfully detected by the RB module.

These settings are amended based on the generated improvement information. However, the error in the setting of the CT secondary nominal current is not identified since there is no corresponding rule for checking CT settings in the rule base. As a result, the amended setting file, although still containing an error, is considered to be correct by the RB module and forwarded to the MB module, where simulation-based validation is conducted and incorrect operations are identified. In the remainder of this section, detailed study of such a case using PPST is provided.

In this study, the same circuit used in the previous case, GREN41-SUND42-1, as shown in Figure 6.3 has been used as in Section 6.3. IED 1 and IED 2 are commercially available IEDs [Als11b] used at each end of the feeder configured as a blocked distance protection scheme, and they are installed at nodes GREN41 and SUND42 respectively.

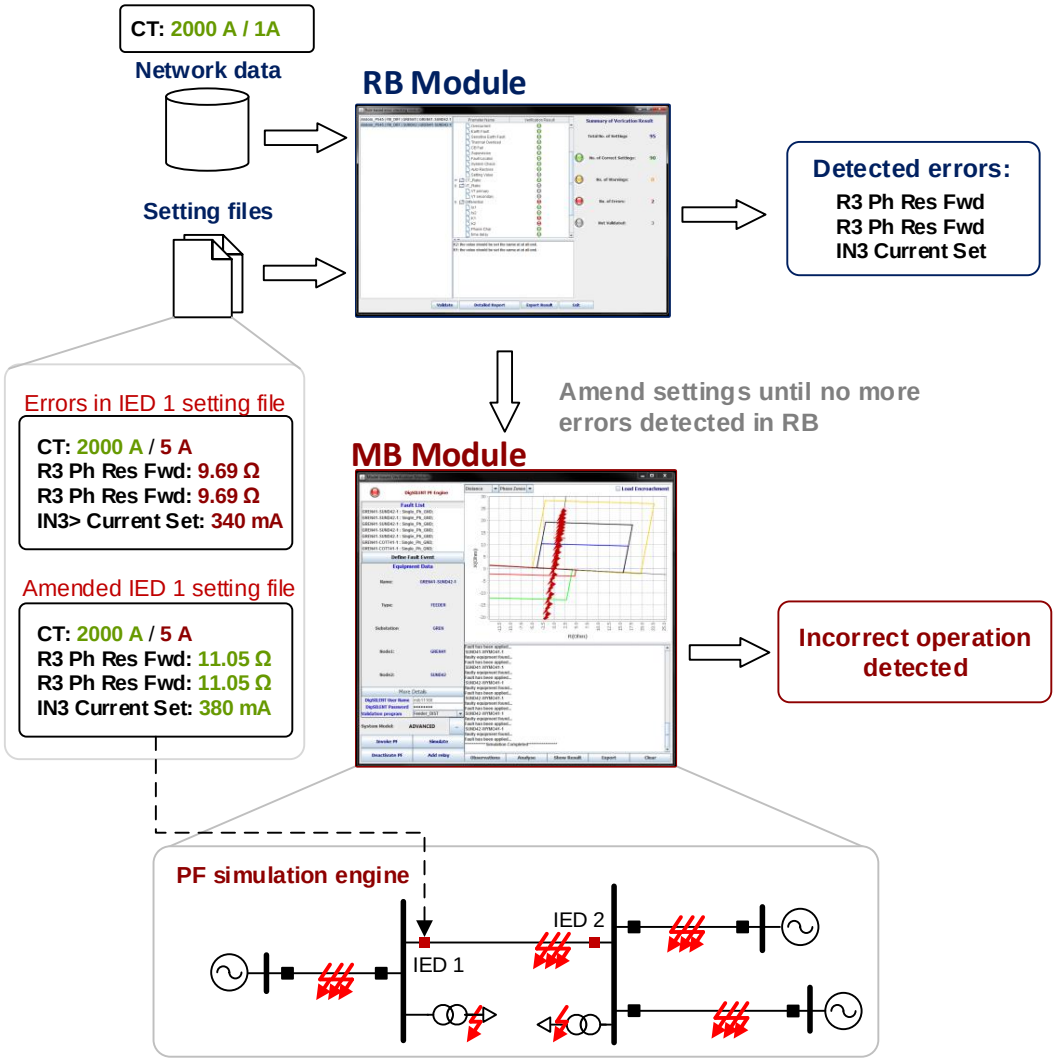


Figure 6.10: Overview of the case study of validating a distance protection scheme

Setting	Description	Value
CT primary	The setting of CT primary nominal current	2000 A
CT secondary	The setting of CT secondary nominal current	5 A
R3 Gnd Res Fwd	Ground Zone 3 forward resistive reach	9.69 Ω (secondary)
Z3 Gnd Angle	Setting of line angle for Ground Zone 3	84°
R3 Ph Res Fwd	Phase Zone 3 forward resistive reach	9.69 Ω (secondary)
Z3 Ph Angle	Setting of line angle for Phase Zone 3	84°
IN3 Current Set	Pick-up setting for third stage earth fault overcurrent element.	340 mA (secondary)

Table 6.6: The description of settings being investigated and their original configured values [Als11b]

6.4.1 RB Validation

Each of the IEDs in the protection scheme contains 181 settings that are considered by PPST. There are 218 rules defined in the rule base for validation of these settings. As in the previous case study, a subset of settings has been selected for demonstration, and the description of these settings and their originally-configured values are provided in Table 6.6.

The settings have been validated using these rules and the results are shown in Figure 6.11. The rules that are associated with these settings are provided in Appendix B.2.2. As it can be seen, there are 181 settings in the setting file being assessed, among which 167 settings are considered correct, 3 errors are detected, 11 settings are not validated, and no warnings are identified. As noted previously, the settings not validated include parameters such as CT and VT primary and secondary nominal values, which are not covered in the policies. The details on the detected errors and the recommendations for rectification/improvement are summarised in Table 6.7. Figure 6.12 shows an example of the detailed information provided for "R3 Ph Res Fwd" in the user interface, which suggests that the detected error is due to the present setting (9.690 Ω) not providing sufficient resistive fault coverage; with a suggested setting value (10.986 Ω) being provided to address this shortcoming.

As mentioned previously, these detected errors are configured based on now-

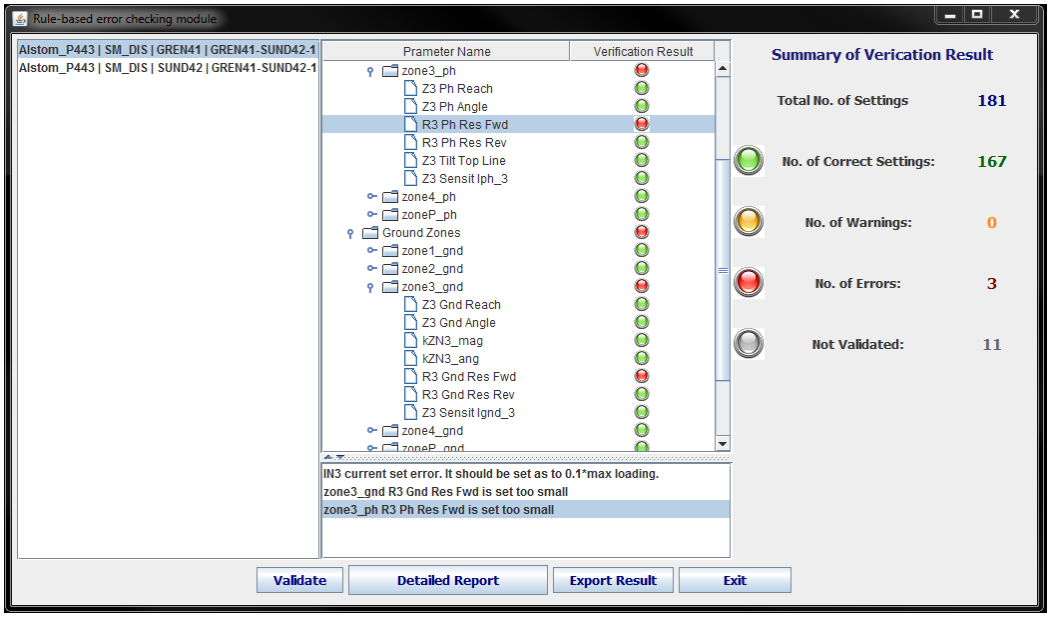


Figure 6.11: The RB validation results for distance protection

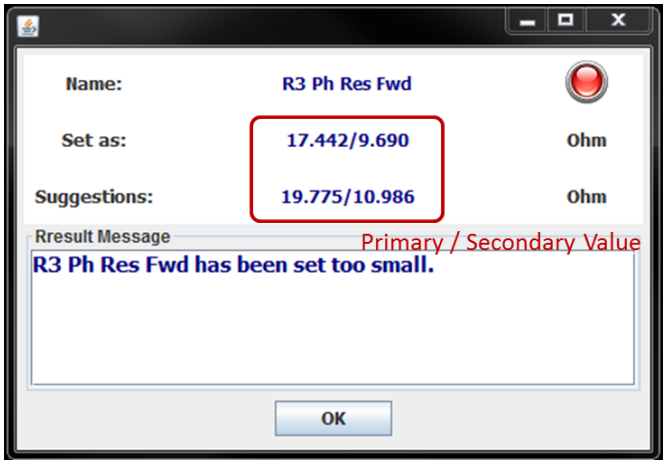


Figure 6.12: The details on the identified errors

Result	Setting	Detailed message
Error	R3 Gnd Res Fwd	Is set too small, failing in providing maximum resistive fault coverage. Suggested setting: 10.986 Ω (secondary).
Error	R3 Ph Res Fwd	Is set too small, failing in providing maximum resistive fault coverage. Suggested setting: 10.986 Ω (secondary).
Error	IN3 Current Set	Should be set as to 10% of maximum loading. Suggested setting: 7600 A (primary)/0.38 A (secondary).

Table 6.7: Identified errors in RB module and generated suggestions

obsolete system conditions and policies. In the past, it was advised that zone 3 resistive reach be set more conservatively (i.e. smaller) to avoid mal-operation during heavy loading conditions, since the potential inaccuracies of the physical devices (such as CT, VT, and the relays) were assumed to be larger in the past. Modern devices tend to offer better accuracy, so the setting policies have been updated to allow the resistive reach to be set with a larger value to provide better sensitivity to resistive faults. In this case, "R3 Ph Res Fwd" and "R3 Gnd Res Fwd" are considered to be not adequate by the existing policies since they do not offer sufficient resistive fault coverage according to the updated policies. The error of "IN3 Current Set" is caused by a change in the maximum loading condition. Historically, the maximum loading was considered to be 6800 A per phase for 400 kV networks, but this has subsequently increased to 7600 A. The setting of "IN3 Current Set" is required to be 10% of the maximum loading; accordingly, the presently-configured value cannot fulfil this criteria due to the increased assumed maximum loading value.

The identified settings are amended based on the generated messages and validated by the RB module again, and after this subsequent analysis, no errors are detected. As mentioned previously, the error in the setting of the CT secondary nominal current is still not detected.

6.4.2 MB Validation

The amended settings are then inserted to the MB module for simulation-based validation, where the CT settings data from the setting file (rather than from the network data) are used for configuring the IED model. The MB module interface is shown in Figure 6.13, where the details of the simulation process are provided. The settings are validated using a number of pre-defined validation templates as shown in Table 6.8. In these templates, a network model with standard type (as introduced in Chapter 5) incorporating the main protected circuit, plus the adjacent-connected circuits, as shown in Figure 6.14 is used and the faults applied within these templates are also detailed in Table 6.8, where the mentioned F1 and R1 branches are illustrated in Figure 6.14. For feeders, faults at various locations, with a step of 2% of the line length (this is configurable), are applied along the line. The 2% fault step size is acceptable as the tolerance of zone reaches is larger than this value (typically 5%). The details of the equivalent sources in the populated network model are provided in Table 6.9 and the configuration of the transformer models used to represent the local and remote parallel-connected transformers is provided in Table 6.10. The transformer models used are of two-winding type with primary and secondary voltage of 400 kV and 132 kV respectively and a rating of 240 MVA. In this case study, the fault contributions from the LV network are neglected. The details relating to how the model is constructed are presented in Appendix A.

These validation templates containing over 500 fault events are simulated as shown in Figure 6.13. The operation details of the protection scheme in each simulated event is recorded and can be viewed as shown in Figure 6.15. On the left hand side, all simulated fault events are listed; in the centre of the window is the summary of operation details of key elements that are most relevant to the distance protection function, where the tripping action and time (in the unit of seconds) of each protection element are provided. In the shown example, a Ph-Ph-Ph fault is applied at 69% of the length of the line SUND42-WYMO41-1 from SUND42 end, and phase zone 1 (zone1_ph), zone 2 (zone2_ph) and zone 3

Validation template	**Description**
Dist_Pro_1ph	Ph-E faults at protected branch
Dist_Pro_3ph	Ph-Ph-Ph faults at protected branch
Dist_F1_1ph	Ph-E faults at F1 branches
Dist_F1_3ph	Ph-Ph-Ph faults at F1 branches
Dist_R1_1ph	Ph-E faults at R1 branches
Dist_R1_3ph	Ph-Ph-Ph faults at R1 branches
Dist_Loc_Tx	Ph-E and Ph-Ph-Ph faults at low voltage side of the local transformer
Dist_Rmt_Tx	Ph-E and Ph-Ph-Ph faults at low voltage side of the remote transformer

Table 6.8: Validation templates for feeder distance protection

Node	Z_{eq1} **and** Z_{eq2} **(Ω)**	Z_{eq0} **(Ω)**
SUND41	8.254	8.061
STAY42	13.364	12.346
COTT41	6.511	2.911
WYMO41	8.089	8.073

Table 6.9: Equivalent source impedance in the network model

Parameter	**GREN41 end**	**SUND42 end**
R_1 (%)	0	0
X_1 (%)	6.413	7.424
R_0 (%)	0	0
X_0 (%)	5.740	7.176

Table 6.10: Configuration of local and remote transformers

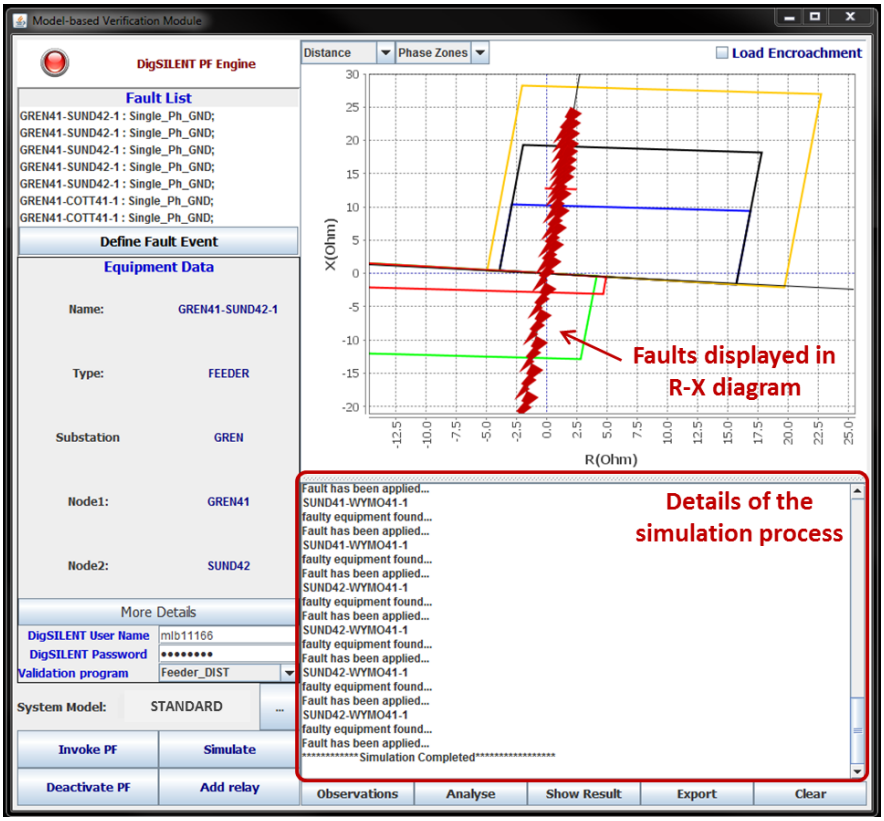


Figure 6.13: The MB validation for distance protection

(zone3_ph) have all tripped with various time delays. The zones with a time delay of 9999.999 s mean these elements did not detect the fault. From this simulated event, an incorrect operation can be identified as zone1_ph has reached to F1 branches which is not desirable.

The large amount of simulation results (from more than 500 events) are analysed automatically. This has been conducted in this study using the rules presented in Appendix B.4.2, and a summary of the analysis results are presented in Figure 6.16, which shows that incorrect operations in six out of eight validation templates have been detected. The abnormal operations of IED 1, detected in each of the individual validation templates, are summarised in Table 6.11.

From Table 6.11, it can be concluded that all of the incorrect operations have a common feature, i.e. overreaching for faults that they are not supposed to react to. Such abnormal operations are caused by incorrect setting of the CT ratio, resulting in the actual zone reaches being significantly larger than the reaches should be. Table 6.12 shows the designed and the implemented zone reaches

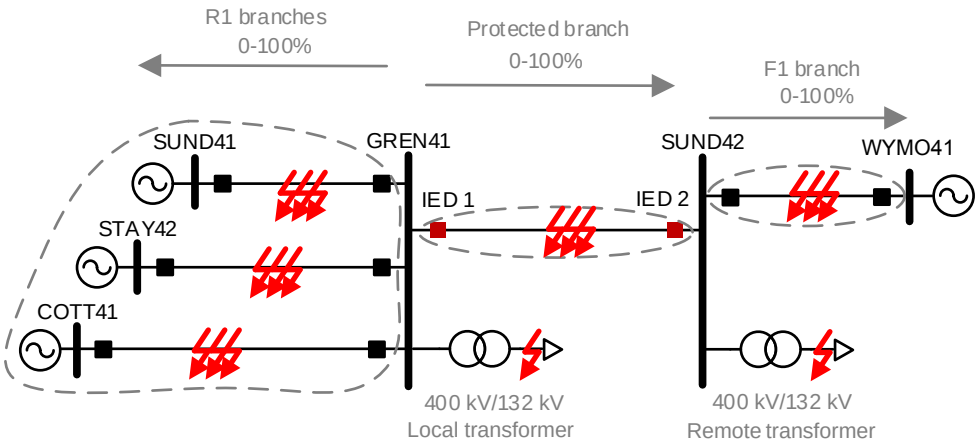


Figure 6.14: The network model for the validation of distance protection

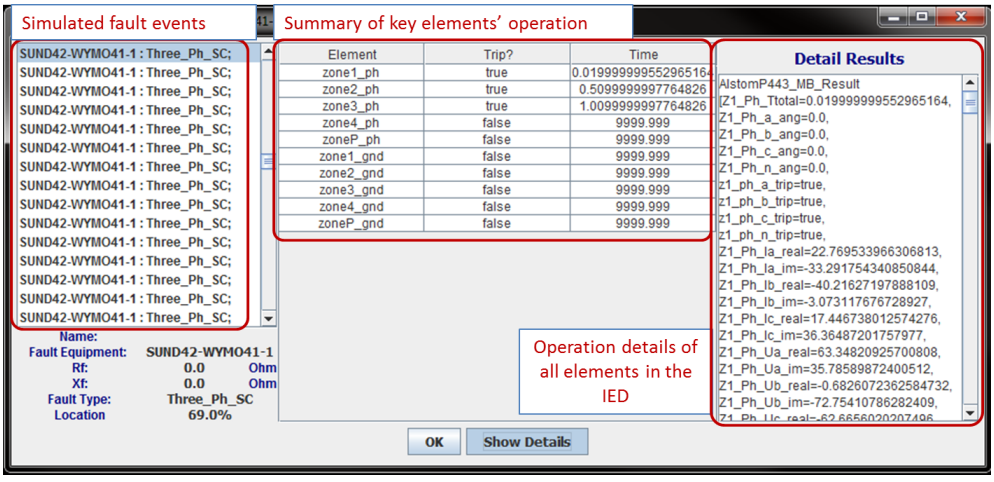


Figure 6.15: Protection operation details under simulated events

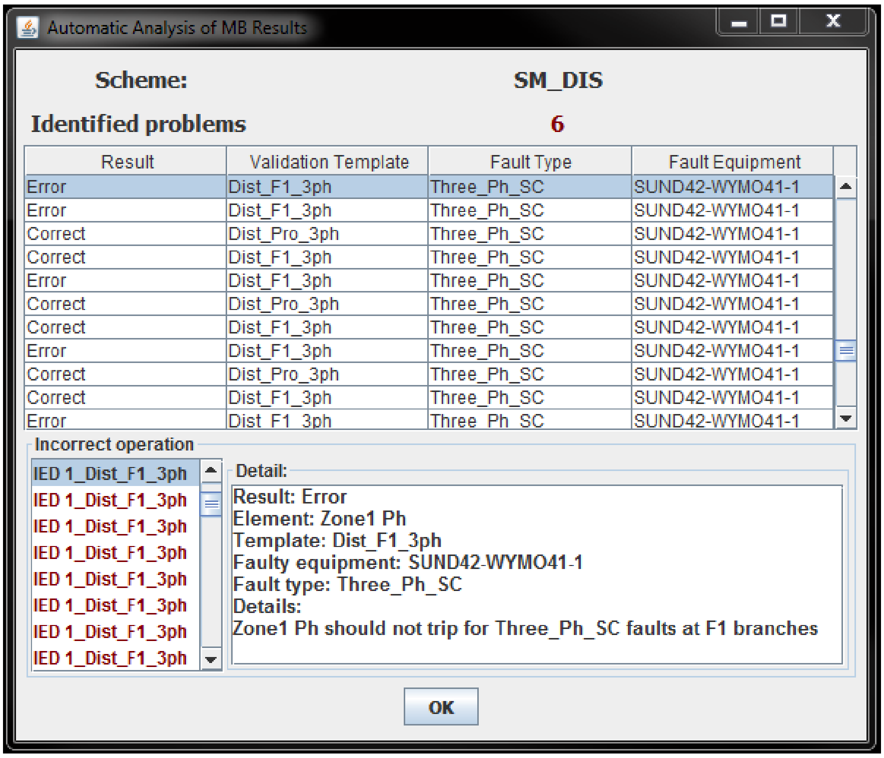


Figure 6.16: MB validation results

Validation template	Abnormal operation identified
Dist_Pro_1ph	Zone 1 gnd trips for faults beyond 85 % of the the line.
Dist_Pro_3ph	Zone 1 ph trips for faults beyond 85 % of the the line.
Dist_F1_1ph	Zone 1 gnd trips for faults at the F1 branches; Zone 2 gnd trips for faults beyond 80% of F1 branches.
Dist_F1_3ph	Zone 1 ph trips for faults at the F1 branches; Zone 2 ph trips for faults beyond 80% of F1 branches.
Dist_R1_1ph	Zone 4 gnd become activated for faults beyond 85% of the R1 branches.
Dist_R1_3ph	Zone 4 ph become activated for faults beyond 85% of the R1 branches.

Table 6.11: The detected incorrect operations in MB validation

Setting	By design	Implemented
CT	2000 A / 1 A	2000 A / 5 A
Zone 1 reach	10.22Ω/5.68Ω	51.12Ω/5.68Ω
Zone 2 reach	19.15Ω/10.64Ω	95.76Ω/10.64Ω
Zone 3 reach	28.13Ω/15.63Ω	140.67Ω/15.63Ω
Zone 4 reach	12.78Ω/7.10Ω	63.90Ω/7.10Ω

Table 6.12: The designed and implemented values the distance protection settings

(both phase and ground zones) using both primary and secondary impedance values (the VT ratio is 3600). It is clear that while the theoretically-correct values and those implemented are the same, the actual implemented reaches using primary values are five times the correct reach values, thus leading to the potential for mal-operations detected by the tool using the MB module and more meaningful diagnostic and remedial suggestions could be developed.

From the overreaching elements, the associated settings can be located, from which the errors in the conversion factors for primary and secondary values can be identified. This would allow the actual error in the CT ratio to be diagnosed. In the future, rules could be further developed so that more detailed heuristics can be provided for easier error location.

In the presented scenario, although the error in CT ratio is simple, it could be overlooked (as happened in actual practice before) and lead to failures of the protection system. The provision of the MB module clearly allows such "hidden" problems to be detected, which would then permit the "missing" rules to be included in the RB module for future and enhanced validation functionality of the tool.

6.4.3 Further Investigations

The same network arrangement and protection scheme have been further investigated with the CT ratio setting error presented in the previous section corrected. The MB validation process was repeated and additional problems were detected in the templates Dist_F1_1ph and Dist_F1_3ph, where zone 2 elements in IED 1 op-

erated for faults beyond 80% of the line SUND42-WYMO41-1 from SUND42 end. This is problematic as the zone 2 elements in IED 1 may overlap zone 2 elements in the protection device at SUND42 end protecting the line SUND42-WYMO41-1 (referred as the downstream IED). This means that IED 1 may operate at the same time as the downstream IED in practice or even faster (depending on the actual time needed to operate the circuit breakers), potentially resulting in the unnecessary disconnection of the line GREN41-SUND42-1. In the setting policies, it is only required that the zone 2 reach should be set between 125%-150% of the protected line's impedance, and IED 1 has been set as 150% as required in this case. However, the issues relating to the potential unnecessary disconnection are currently not incorporated in the RB module. To address this problem, one solution is to reduce the zone 2 settings in IED 1 from 150% of the protected line's impedance to below 131% so that the downstream IED can operate before IED 1 for the aforementioned faults.

Further investigations have been conducted by varying the lengths of the lines to test how the protection system will operate when potential changes are made to the network. It has been found that when the length of the line SUND42-WYMO41-1 reduces from 17.99 km to 14.30 km (with all the other lines unchanged), the zone 2 settings of IED 1 will have to be reduced below 125% of the protected line's impedance in order to avoid overlapping zone 2 elements in the downstream IED. However, this is presently not allowed by the setting policies. In such cases, specific criteria for setting zone 2 reaches need to be established and added to the RB module in order to cope with this type of network arrangements in the future.

6.5 Conclusions

The validation of protection settings is clearly a challenging task, given the significant number of protective devices and the associated settings available. In this chapter, it has been demonstrated how such challenges can be overcome by the developed PPST system, which is implemented based on the methodology pre-

sented in this thesis. The functionalities and the associated benefits offered by PPST have been demonstrated through two illustrative and realistic case studies.

The first case study demonstrates the use of PPST for the validation of the feeder differential protection, where 95 settings in each IED (giving a total of 190 settings in the two IEDs in the scheme) have been interrogated by the RB module. For the protection scheme being investigated, 89 rules have been implemented for comprehensive checking of the IED type application, functional configuration, settings calculation, and coordination. Human errors have been deliberately introduced, which result in the violation of setting policies. These errors are successfully detected by PPST, which allows amendment of the settings to be made. The updated settings are then checked in the MB module, where the worst-case scenarios for the protection scheme have been simulated. The results show correct operation of the scheme, which therefore verifies the RB results and suggested and implemented amendments to the settings.

The second example, which is used to illustrate two main aspects of PPST functionality, firstly presents a scenario where settings based upon obsolete setting polices and system conditions do not comply with the updated policies. The RB module interrogated 181 settings in each IED (giving a total of 362 settings checked) and the errors are successfully detected. Secondly, it is also demonstrated how under some circumstances, the RB module may not be capable of anticipating and detecting all problems, which could lead to protection failure. In the second element of the case study, an error in the CT ratio setting is introduced which is not detected by the RB module - this is reflective of an actual historical incident which led to a blackout of a major part of a power system. This specific problem, while "missed" by the RB policy-based validation process, is detected by the simulation-based validation process adopted using the MB module. A number of potential problems that are not detected by the RB module have also been identified in the further investigation activities using the MB module. The detected of "hidden" problems during simulation allows the review and improvement of the rule base to be implemented to enhance the functionality and breadth of the system for future validation exercises.

Through the second case study, it has been demonstrated that the provision of the MB module allows potential problem instances that are not defined in the RB module to be detected through simulation, which offers enhanced reliability than systems based on a single RB approach. Compared to existing MB systems, which require significant manual input for the validation task, it has been demonstrated that the entire settings validation process can be automated in PPST, and the enhanced automation is facilitated by the provision of the RB module for automated analysis of simulation results. This proves that the combined RB and MB approaches are effective in complementing each other, offering a satisfactory solution for the settings and performance validation tasks.

Chapter 7

Conclusions and Further Work

7.1 Conclusions

The validation of protection settings and performance is essential to ensure the reliable operation of protection and of course the protected power systems. However, the evolution and increasing complexity of the network and the large number of protective devices (and their associated settings) make such a task extremely challenging. Existing relevant software systems have a number of shortcomings: the systems performing settings calculation are not readily suitable for the validation task; existing systems that can be used for the settings validation task are mainly MB systems and require significant manual input during the validation process (e.g. for construction of network models, configuration of protection IED models using the settings to be validated, analysis of simulation results, etc.). Furthermore, no system is available that can perform checking against setting policies and indeed the validation of the setting policy itself.

In this thesis, the aforementioned problems have been addressed and the results of research into a methodology for automatic and comprehensive validation of protection settings has been presented. A hybrid RB and MB approach has been adopted for the validation task. The RB module checks the settings against the rules translated from setting policies. Experts' experience and knowledge are also included to perform plausibility checks. The validation rules can be

categorised into four types, focusing on different validation aspects, i.e. the application of the IED types, the functional configuration, the settings calculation, and the coordination with other protective devices in the same scheme. The RB validation ensures the settings conform to the requirements specified in the setting policies.

The shortcoming of the RB approach is the possibility that some problem instances are not included or that there may be some inherent deficiencies in the setting policies. The MB module has therefore been developed and included as a further means of performance checking through the use of simulation-based validation. The functional knowledge included in the models allows the system to react to a wide range of conditions including those that may be unanticipated during original configuration and implementation of the protection system and its settings. A mechanism has been developed that allows the automation of the entire simulation process to avoid the requirement for significant manual input as is often the case in existing systems similar systems that have been developed. This is achieved by the interaction with a commercially available PowerFactory simulation engine to leverage its internal functions and data for validation purposes.

However, the disadvantages of using a single MB approach are the difficulties in incorporating setting policies during the validation process and the significant manual input required for analysing simulation results. Such issues have been addressed using the RB module, which is a more suitable option for checking settings against policies and allows automated analysis of MB simulation results. The combined RB and MB approaches have proven to be effective in complementing each other for the settings validation task, offering a satisfactory solution and this has been demonstrated using two case studies.

The proposed methodology has been implemented as an intelligent system (known as PPST) and tested using data from the GB transmission system. It has been demonstrated that PPST is capable of automating the entire settings validation task, identifying hidden errors and providing sufficient information for remedying any identified issues. It has also been demonstrated that, in some

circumstances, the RB module may fail to detect specific problems that are not covered in the setting policies, but these can be identified in the MB module, so that the missing scenarios can be added to the rule base for future validation task.

During the research work, it has been realised that one of the key challenges in developing the intelligent system for automatic protection settings validation is the existing way of managing settings data in proprietary formats, which are difficult to access and manipulate. Such difficulties are also experienced by any systems that require the use of protection settings data, which can result in a significant burden being placed on the system development and maintenance functions. Furthermore, the need for proprietary software tools to configure protection settings also leads to a complex engineering process for the protection and automation systems.

In this thesis, a novel solution to these challenges has been proposed and demonstrated through the use of the data model provided by the IEC 61850 standard with the SCL format to represent protection settings data. Based on this common representation method, a novel IED configuration process is proposed, which is significantly streamlined and efficient compared with the existing approaches. It has been shown that the SCL-based protection settings format is easier to interpret and manipulate using software, which significantly reduces the burden of designing, implementing, and maintaining protection schemes. The design of the open platform tool (known as PSCT) that can automatically convert existing settings data between proprietary formats and the SCL-based format has been presented, which provides support for network operators to migrate to the proposed approach (based on standardised settings) from existing approaches.

Adoption of the recommendations and design approaches presented in this thesis would shift protection systems from being largely single-vendor solutions to becoming efficient and truly open platforms, capable of supporting future intelligent applications and tools such as automated protection settings validation (as reported in this thesis), diagnostics, and adaptive protection schemes.

7.2 Future Work

7.2.1 Enhancement of the MB Module

In the existing MB module, only limited validation templates for each protection scheme have been defined, and the system events simulated are mainly fault events. The next stage of the work would investigate the definition of further validation templates to cater for a wider array of tests. This can be achieved by embedding experienced engineers' knowledge within the new template definition process, so that other types of system events (e.g. overloading, power swings and other transient phenomena) can also be included in the simulation and the performance of the protection under a wider range of circumstances can be analysed and verified.

Furthermore, the models used in the MB module can be further extended and improved, which could include the use of converter models to simulate the protection performance in power systems that are dominated by non-synchronous generations in order to assess the validity of existing setting policies in the future scenarios; the improvement of the equivalent network models so that they can better reflect the actual situation where the network is highly interconnected; and the detailed and more accurate modelling of protection components (e.g. CTs) so that more problem instances (e.g. CT saturation) that may occur in a physical system can be identified in the MB simulation process.

The existing rules for analysing simulation results have been proven to be very useful when there are large amounts of simulation results returned. However, existing analysis rules cover only the fundamental checks to establish whether any major violation of expected performance are experienced - more refined rules that could check for more subtle problems should be developed and incorporated in the future, so that more meaningful diagnostic and remedial suggestions could be provided when incorrect operations are detected.

7.2.2 Migration of System from Off-Line to On-Line Mode of Operation

The network data currently used is stored in the form of CSV files, i.e. the system is running in what could be termed as an off-line mode. The main disadvantage of such an arrangement is that the data is not updated in real time, resulting in potential failures in reflecting the actual prevailing network operating conditions and topology.

The next step of the work can look at interfacing the system to on-line data sources (e.g. SCADA systems) that can provide real time data of the network, so that the most timely data is used for settings validation and the validation process can be triggered automatically whenever changes in the network are identified.

7.2.3 Further Development of the Prototype Tool for Industrial Application

The ultimate objective of the work is to deliver the intelligent system for industrial applications as "business as usual". In order to achieve this, the prototype is required to be further developed, refined and comprehensively tested.

The existing prototype only supports a limited range of IED types and protection schemes, and only considers feeders and transformers in the network during the validation process. Further development work is required to extend the support for a wider range of IED types and protection schemes, and to include more network components in the validation to better reflect the actual operating arrangements.

Another important aspect for future improvement is to refine the design of the tool, so that it can be more readily extended, i.e. easier to extend support for new IED types and protection schemes. This is important to make sure the system can be properly maintained in the future.

7.2.4 Comprehensive Study of the Settings for Existing and Future Systems - Roll out of the Process to the Entire System

Once the development, refinement and test of the prototype system are complete, a comprehensive study of the existing settings data in the GB transmission network can be performed. This allows the detection of any existing unknown errors and potential problems with existing policies.

With the MB module, studies on how the protection system will behave in future network scenarios (i.e. with variable fault levels, increased loading, changes of generation patterns, etc.) can be undertaken, and this would be facilitated by the incorporation of converter models as mentioned in Section 7.2.1. Such studies can be of significant benefit for understanding the impact of the changes of the network on the protection settings, and they can also help to establish new setting policies for the future network.

7.2.5 RB Validation Based on Common Protection Settings Data

Since the existing protection settings are stored in proprietary formats and the existing protection IED models only support proprietary settings, the presented methodology and the current version of the prototype have been developed based on the proprietary approaches.

Future work can investigate developing an RB validation module based on common protection settings. This can be facilitated by the settings conversion tool as presented in Chapter 4. The key benefits of conducting such work is to further prove the feasibility of the proposed approach, and the system, when based on common settings, will be easier to be adopted for used by different network operators (with different policies) due to the ease with which the rule base may be updated.

Appendix A

Creation of Equivalent Network Models in the MB Module

For the MB validation of protection settings, equivalent network models are used in the PPST system. There are two main elements involved when developing equivalent models. Firstly, the level of detail within the network model is determined, i.e. identifying which parts of the actual network should be included in the model and which part should be represented using equivalent components. In Chapter 5, three types of network models (i.e. simplified, standard and advanced) for testing different protection schemes have been introduced. Secondly, the equivalent sources must be configured so that they can simulate certain system conditions (e.g. maximum and minimum fault currents). This is achieved by proper selection of the internal impedances of equivalent sources. In the following sections, examples relating to how equivalent components (including equivalent sources) in the various types of network models are established are presented.

A.1 Creation of Simplified Network Models

The simplified network model is used for the validation of differential, earth fault and phase overcurrent protection. Taking the validation of protection schemes at the feeder GREN41-SUND42-1 (shown in Figure B.1 in Appendix B) as an

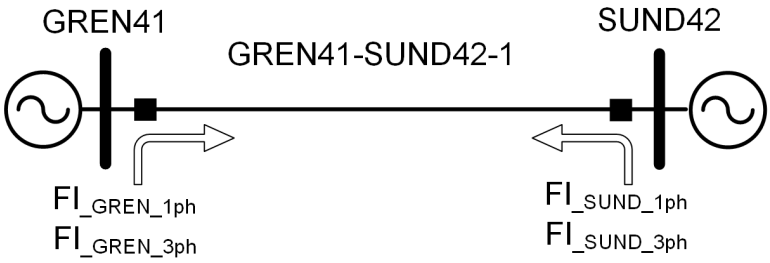


Figure A.1: Simplified model for GREN41-SUND42-1

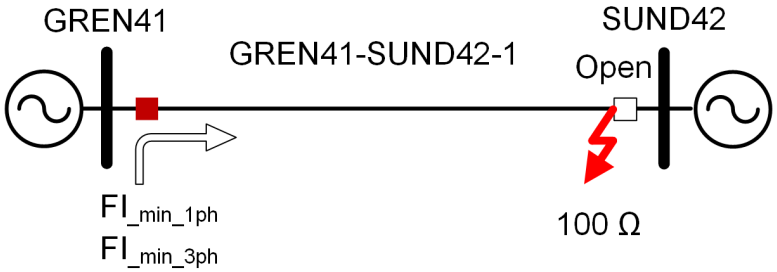


Figure A.2: Minimum fault condition with respect to GREN41 end

example, the corresponding simplified model is shown in Figure A.1. The sources at the nodes GREN41 and SUND42 can be configured to simulate various system conditions. For example, for the validation of the sensitivity of the differential protection scheme, the model is required to be configured to simulate the minimum fault level condition, which is defined by the scenario where a 100 Ω resistive fault occurs at the remote end (with respect to the relay being analysed) with local minimum fault infeed (established automatically from the database in PPST) and the remote end circuit breaker open. With respect to the node GREN41, the minimum fault condition can be adopted by the configuration shown in Figure A.2, where $FI_{\_min\_1ph}$ and $FI_{\_min\_3ph}$ are the minimum single-phase and three-phase fault infeed that are adopted from the fault level survey conducted by the network operators (in the case of National Grid, this is done on annual basis [Nat14]). The remote end circuit breaker is open, so there is no fault infeed from SUND42 when a 100 Ω resistive fault occurs at the end of the feeder (i.e. the SUND42 end). The internal positive (Z_{eq1}) and zero (Z_{eq0}) sequence impedance of the equivalent source at GREN41 can be determined by the following equations (with equations A.2 and A.3 referring to Figure A.3):

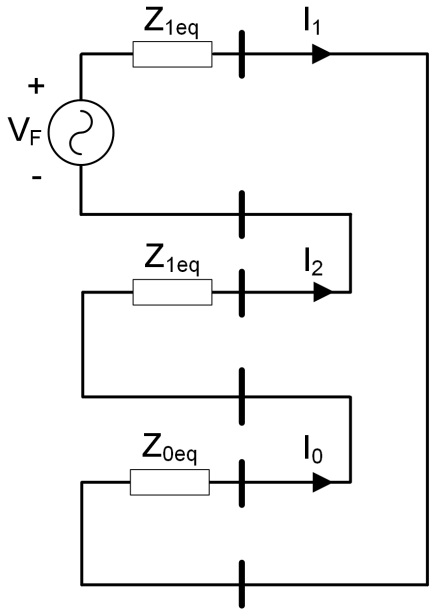


Figure A.3: Positive, negative and zero sequence network connection during a Ph-E fault

$$Z_{eq1} = \frac{V}{\sqrt{3} \times FI_{\_min\_3ph}} \tag{A.1}$$

$$FI_{\_min\_1ph} = 3 \times I_1 = \frac{3 \times V_F}{2 \times Z_{eq1} + Z_{eq0}} \tag{A.2}$$

$$\begin{aligned} Z_{eq0} &= \frac{3 \times V/\sqrt{3}}{FI_{\_min\_1ph}} - 2 \times Z_{eq1} \\ &= \frac{\sqrt{3} \times V}{FI_{\_min\_1ph}} - 2 \times \frac{V}{\sqrt{3} \times FI_{\_min\_3ph}} \end{aligned} \tag{A.3}$$

where V is the line voltage; V_F is the pre-fault phase voltage; and it is assumed that positive and zero sequence impedances are identical [GSO12].

Table A.1 provides summer minimum fault level data at node GREN41, where details on the fault contributions from connected equipment are presented.

From the data provided, $FI_{\_min\_1ph}$ and $FI_{\_min\_3ph}$ can be calculated as:

$$FI_{\_min\_1ph} = 21.250 - 6.233 = 15.017kA$$

Node	Equipment	$FL_{1ph}(kA)$	$FL_{3ph}(kA)$
GREN41		21.250	25.090
	GREN41-SUND41-1	6.684	8.863
	GREN41-SUND42-1	6.233	8.311
	...	...	...

Table A.1: Summer minimum fault level data of GREN41 node

$$FI_{\_min\_3ph} = 25.090 - 8.311 = 16.779kA$$

Using equations A.1 and A.3, Z_{eq1} and Z_{eq0} can be calculated, which are 13.764 Ω and 18.608 Ω respectively (assuming a line voltage of 400 kV).

The same procedure can be repeated for the determination of the minimum fault conditions for the protective device at SUND42 end, and the protection scheme is required to detect faults under both scenarios. For testing the stability of the protection scheme, the model needs to be configured to simulate maximum external fault condition. Assuming the single-phase and three-phase maximum fault infeeds at a node are FI_{max_1ph} and FI_{max_3ph} respectively, the corresponding positive sequence and zero sequence impedances can be calculated using equations A.1 and A.3 by replacing $FI_{\_min\_1ph}$ and $FI_{\_min\_3ph}$ with FI_{max_1ph} and FI_{max_3ph} respectively.

A.2 Creation of Standard Network Models

The standard network model incorporates the protected feeder and the adjacent circuits that are connected to the nodes of the protected feeder. There are also two representative transformers included, one at each end, to represent the minimum impedance to the LV networks through the parallel-connected transformers at each end. This type of model is used for validating distance protection schemes in the developed PPST system. Figure A.4 shows the standard model for validation of the distance protection scheme applied to the feeder GREN41-SUND42-1 as shown in Figure B.1 in Appendix B.

The internal positive and zero sequence impedances of the equivalent sources

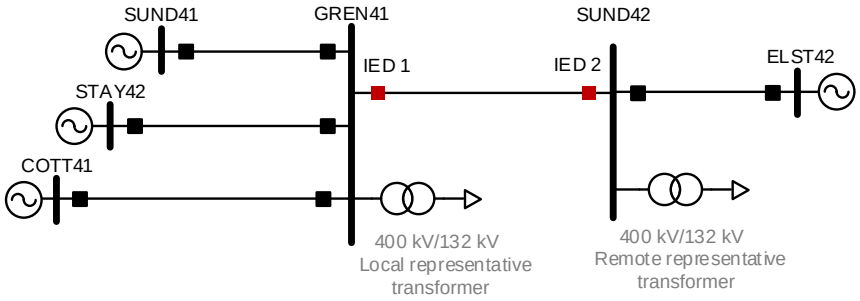


Figure A.4: An example of standard model

at node SUND41, STAY42, COTT41 and ELST42 can be derived by the same methodology as introduced in Section A.1 using fault level data at each of these nodes. Taking the node COTT41 as an example, the fault level data at the node is shown in Table A.2.

Node	**Equipment**	$FL_{1ph}(kA)$	$FL_{3ph}(kA)$
COTT41		45.763	37.963
	COTT41-GREN41-1	2.280	2.492
	COTT41-STAY42-1	4.526	4.354
	...	...	...

Table A.2: Fault level data of COTT41 node

The fault infeeds to the feeder COTT41-GREN41-1 through the node COTT41 are considered to be:

$$FL_{COTT\_1ph} = 45.763 - 2.280 = 43.483kA$$

$$FL_{COTT\_3ph} = 37.963 - 2.492 = 35.471kA$$

Using equations A.1 and A.3 with $FI_{\_min\_1ph}$ and $FI_{\_min\_3ph}$ substituted by FL_{COTT_1ph} and FL_{COTT_1ph} respectively, the internal positive and zero sequence impedance of the equivalent source at COTT41 can be adopted as 6.511 Ω and 2.911 Ω respectively (assuming a line voltage of 400 kV).

The fault level data used for developing the network model is derived from fault level simulations conducted by National Grid using a detailed full GB network model. The actual system is a highly interconnected network, while

in the standard network model as discussed in this section, a number of non-interconnected equivalent sources are used to represent the infeeds of the external network sections to the main infeed points represented in the standard network model. In practice, interconnections (e.g. through parallel paths that are not faulted) between sources may act to increase/decrease fault levels in the full GB network model.

These effects may not be modelled in the standard (reduced) network model used in the developed system. However, it is proposed that such an approximation is acceptable, since the standard network model is used for testing distance protection schemes, which operate based on the ratios of measured voltages and currents, and are therefore largely independent of fault levels and any variations therein. Furthermore, faults applied in the associated validation templates all assume zero impedance short circuits, thus any effects due to changes in fault level upon the zone reaches will be negligible. Future work should look at incorporating representative elements in the network model to emulate the interconnection effects so that the model can better represent the actual scenarios.

For testing of whether the distance protection zones will reach to the LV networks through transformers - which is undesirable - a method has been developed to represent the minimum impedance in this context, i.e. for a fault that is "inside" a transformer, that may be measured by the distance protection using a representative transformer model. From analyses of the protection policies and discussions with experts, there is some uncertainty in the exact optimal physical location of the maximum reach of the distance relays (e.g. reaching to cover the primary winding, into the secondary winding, the entire transformer but not beyond LV terminals, etc.). Furthermore, this situation is complicated by the differences in transformer types, configuration and whether multiple transformers from a remote busbar may be operating in parallel or not. This will clearly change the fault current paths and apparent impedance measured by a remote relay.

In the developed system, this complexity has been dealt with to an extent, but further work would remain to be carried out to ensure that the system is com-

pletely accurate and aligned with policies and experts' needs for this complicated situation. For now, the worst-case scenario (i.e. the minimum impedance measured by the distance protection for a remote fault at, or inside, a transformer) has been derived from transformers' equivalent circuits as shown in Figure A.5, where a fault occurs at a point between the primary and secondary winding impedances of the transformer with a minimum fault impedance, and all transformers are connected in parallel. As already mentioned, the actual worst-case scenario may be subject to differences in actual transformer types, connections, locations of the faults (e.g. inside the secondary windings), network running arrangements, etc. This situation is an area where future work could be carried out to establish a more comprehensive understanding and modelling of worst-case scenarios to cater for the impact of the various factors on the distance protection reach in this context.

In Figure A.5, Z_{HV} and Z_{LV} are the primary and secondary impedance of the transformer with minimum impedance (assuming Tx_1 in this case), and Z_T is the overall impedance of all other transformers connected in parallel with Tx_1.

The equivalent positive impedance (Z_{eq1}) seen from the HV side of the transformers can be adopted by equation A.4:

$$\begin{aligned} Z_{eq1} &= Z_{HV\_1}//(Z_{LV\_1} + Z_{T\_1}) \\ &= \frac{Z_{HV\_1} \times (Z_{LV\_1} + Z_{T\_1})}{Z_{HV\_1} + Z_{LV\_1} + Z_{T\_1}} \end{aligned} \tag{A.4}$$

where Z_{HV_1} and Z_{LV_1} are the positive sequence impedance of the primary and secondary winding of Tx_1, and Z_{T_1} is the overall positive impedance of all other transformers connected in parallel with Tx_1.

For determination of the equivalent zero sequence impedance (Z_{eq_0}), referring to the sequence network as shown in Figure A.6 (where V_{TH} and I_{TH} are the equivalent voltage and current defined in the Thévenin's equivalent theorem

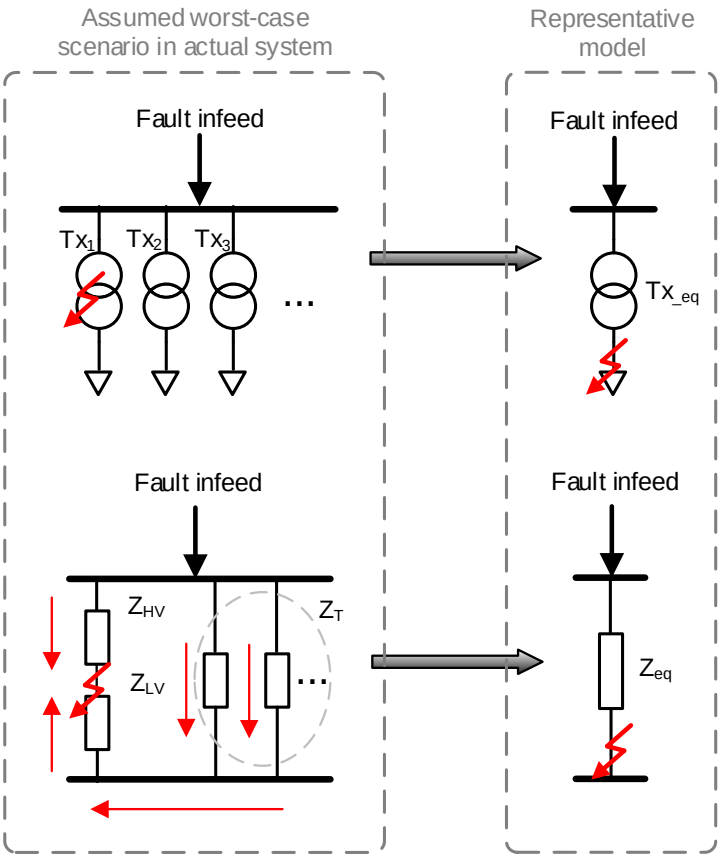


Figure A.5: Representing minimum impedance to LV side using an equivalent transformer

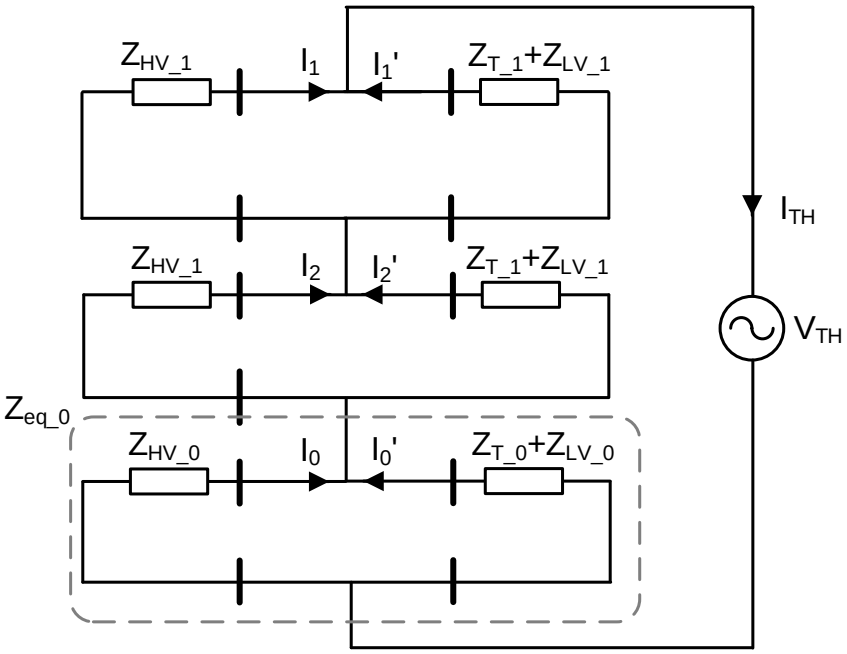


Figure A.6: Sequence network of the minimum impedance scenario

[GSO12]), Z_{eq_0} can be derived using equation A.5:

$$\begin{aligned} Z_{eq0} &= Z_{HV\_0}//(Z_{LV\_0} + Z_{T\_0}) \\ &= \frac{Z_{HV\_0} \times (Z_{LV\_0} + Z_{T\_0})}{Z_{HV\_0} + Z_{LV\_0} + Z_{T\_0}} \end{aligned} \tag{A.5}$$

where Z_{HV_0} and Z_{LV_0} are the zero sequence impedance of the primary and secondary winding of Tx_1 respectively; and Z_{T_0} is the overall zero impedance of all other transformers connected in parallel with Tx_1.

The calculated equivalent positive and zero sequence impedance are used for configuring the representative transformer model. When a fault occurs at the secondary side of the representative transformer, it effectively represents the minimum impedance that the distance protection will see during fault conditions. Therefore, if the distance protection operates for faults at the secondary side of the equivalent transformer, it means that the settings may potentially lead to the protection reaching into LV networks, which is not permissible. Assuming that there are three transformers (with a rated power of 240 MVA) installed at GREN41 end with the data shown in Table A.3.

Parameter	Tx_1	Tx_2, Tx_3
R_1 HV (%)	0.173	0.187
X_1 HV (%)	9.542	10.048
R_1 LV (%)	0.141	0.187
X_1 LV (%)	9.542	10.048
R_0 HV (%)	0.173	0.187
X_0 HV (%)	8.391	9.768
R_0 LV (%)	0.141	0.187
X_0 LV (%)	8.391	9.768

Table A.3: Example transformers data

It can be seen that Tx_1 has the smallest impedance among all transformers, and the associated parameters of Tx_1 as presented in equations A.4 and A.5 can be calculated as:

$$Z_{HV\_1} = 9.544\%$$

$$Z_{HV\_0} = 8.393\%$$

$$Z_{LV\_1} = 9.543\%$$

$$Z_{LV\_0} = 8.392\%$$

The overall positive and zero sequence impedance of Tx_2 and Tx_3 are 20.010% and 19.540% respectively. Therefore, the overall parallel-connected positive and zero sequence impedance are:

$$Z_{T\_1} = 20.010\%/2 = 10.005\%$$

$$Z_{T\_0} = 19.540\%/2 = 9.770\%$$

Using equations A.4 and A.5, Z_{eq1} and Z_{eq0} of the equivalent transformer can be calculated as 6.413% and 5.740% respectively. Table A.4 presents the details of the configuration of the equivalent transformer model using the calculated Z_{eq1}

and Z_{eq0} values.

R_1 (%)	0
X_1 (%)	6.413
R_0 (%)	0
X_0 (%)	5.740

Table A.4: Configuration of the equivalent transformer model

The advanced model has not currently been used in the developed PPST system. However, the principle of developing such a network model is the same as the case for the standard model with equipment at the tertiary level from the protected feeder in both forward and reverse directions also included. As mentioned previously, future work should investigate including equivalent elements in the model to emulate the interconnection effects as in the actual system.

Appendix B

Supplementary Information for Case Studies in Chapter 6

This appendix provides supplementary details for the case studies presented in Chapter 6. Section B.1 presents the circuit data of the network used in the case studies. The settings validation rules and the associated calculation processes are presented in Section B.2 and Section B.3 respectively. In Section B.4, the rules used for automated analysis of MB simulation results are provided.

B.1 Circuit Data for Case Studies

Figure B.1 shows the circuit diagram for the test network in the case studies, and the feeder investigated is GREN41-SUND42-1. The data for the elements shown in the circuit diagram is provided in Table B.1 and Table B.2, and the associated fault levels data is presented in Table B.3. The voltage level of the network is 400 kV and the feeders' data is provided in per unit with a voltage base of V_{base} = 400 kV and an apparent power base of S_{base} = 100 MVA. The transformers are assumed to be with two-winding type, a rating of 240 MVA and primary and secondary voltage of 400 kV/132 kV.

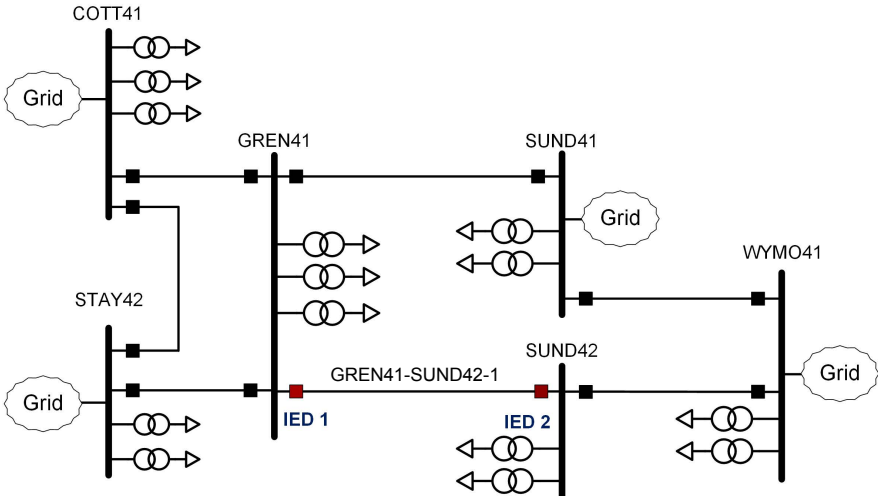


Figure B.1: Network for the case studies

Parameter	**GREN** Tx_1	**GREN** Tx_2, Tx_3	**SUND** Tx_1, Tx_2
R_1 HV (%)	0.173	0.187	0.268
X_1 HV (%)	9.542	10.048	9.895
R_1 LV (%)	0.141	0.187	0.134
X_1 LV (%)	9.542	10.048	9.895
R_0 HV (%)	0.173	0.187	0.268
X_0 HV (%)	8.391	9.768	9.564
R_0 LV (%)	0.141	0.187	0.134
X_0 LV (%)	8.391	9.768	9.564

Table B.1: The data of transformers

Name	**Length(km)**	$R_1(\%)$	$X_1(\%)$	$B_1(\%)$	$R_0(\%)$	$X_0(\%)$	$B_0(\%)$
GREN41-SUND41-1	39.75	0.0723	0.791	23.037	0.352	2.088	14.389
GREN41-SUND42-1	39.96	0.0727	0.795	23.155	0.354	2.098	14.456
GREN41-COTT41-1	129.48	0.229	2.555	75.719	1.126	6.772	47.156
GREN41-STAY42-1	101.83	0.185	2.026	59.022	0.902	5.348	36.851
SUND41-WYMO41-1	18.16	0.020	0.315	11.993	0.117	0.896	7.199
SUND42-WYMO41-1	17.99	0.0195	0.313	11.857	0.116	0.886	7.136
COTT41-STAY42-1	27.70	0.044	0.530	16.733	0.225	1.427	10.324

Table B.2: The data of feeders

Node	**Equipment**	$FL_{1ph}(kA)$	$FL_{3ph}(kA)$
GREN41		21.250	25.090
	GREN41-SUND42-1	6.233	8.311
	Others	15.017	16.779
SUND41		33.303	33.084
	GREN41-SUND41-1	5.104	5.104
	Others	28.199	27.980
SUND42		30.575	30.440
	GREN41-SUND42-1	5.566	5.586
	Others	25.009	24.854
COTT41		45.763	37.963
	COTT41-GREN41-1	2.28	2.492
	Others	43.483	35.471
STAY42		21.490	21.637
	STAY42-GREN41-1	3.759	4.356
	Others	17.731	17.281
WYMO41		35.883	36.712
	SUND42-WYMO41-1	7.314	8.162
	Others	28.569	28.550

Table B.3: Minimum fault levels data and the associated fault contributions from connected elements

B.2 Settings Validation Rules

For simplicity and ease of understanding, the rules are presented in a descriptive fashion in this appendix. An example of how the descriptive rule is represented in source code format is provided in Section 5.3 in Chapter 5. In the execution part ("then" part) of each rule, the validation result (error or warning) is provided, along with a message that specifies the details on the detected problems.

The descriptions of the setting parameters appeared in the rules are provided in Chapter 6. In the rules, further calculations may be involved, and the details relating to such calculations are provided in Section B.3.

B.2.1 Validation Rules for Case Study 1

When	**Then**
Phase Diff is set as Disabled	**Error**: Phase Diff should be enabled for feeder differential protection.

Table B.4: Validation rule for the setting Phase Diff

When	**Then**
Auto-Reclose is set as Enabled	**Error**: Auto-Reclose should be fixed as disabled for feeder differential protection.

Table B.5: Validation rule for the setting Auto-Reclose

	When	Then
1	$I_{s1} < 2.5 \times I_c$	**Error**: I_{s1} should be set as least 2.5 times of the line charging current.
2	$I_{s1} < 10\% \times CT_{sec}$	**Error**: I_{s1} should be set as least 10% of CT secondary nominal current.
3	$I_{f\_min} < 1.5 \times I_{s1}$	**Error**: The minimum fault current should be at least 1.5 times of I_{s1}.
4	I_{s1} is not set the same at all ends	**Error**: I_{s1} should be set the same at all ends.

Note: I_c is the line charging current (Section B.3.1);
CT_{sec} is the CT secondary nominal current.
I_{f_min} is the minimum fault current (Section B.3.2);

Table B.6: Validation rules for the setting I_{s1}

	When	Then
1	I_{s2} is not set as $10 \times I_{s1}$	**Error**: I_{s2} should be set as 10 times of I_{s1}.
2	I_{s2} is not set the same at all ends	**Error**: I_{s2} should be set at all ends.

Table B.7: Validation rules for the setting I_{s2}

	When	Then
1	I_{diff} is minimum ; $I_{bias} < I_{s2}$; k_1 leads to $I_{diff} < 1.2 \times I_{op}$;	**Error**: during minimum fault condition, I_{diff}/I_{op} should be $\geqslant$ 1.2 so as to provide sufficient sensitivity.
2	k_1 is not set the same at all end	**Error**: k_1 should be set the same at all ends.

Note: more details on I_{diff}, I_{bias}, I_{op}, and the definition of rule 1 are provided in Section B.3.3.

Table B.8: Validation rules for the setting k_1

	When	Then
1	I_{diff} is minimum ; $I_{bias} \geqslant I_{s2}$; k_2 leads to $I_{diff} < 1.2 \times I_{op}$;	**Error**: during minimum fault condition, I_{diff}/I_{op} should be $\geqslant 1.2$ so as to provide sufficient sensitivity.
2	k_2 is not set the same at all end	**Error**: k_2 should be the same set at all ends.

Note: details on I_{diff}, I_{bias}, I_{op}, and the definition of rule 1 are provided in Section B.3.3.

Table B.9: Validation rules for the setting k_2

B.2.2 Validation Rules for Case Study 2

	When	Then
1	$R_3 \leq 95\% \times R_{ch\_max}$; $R_3 \geqslant 90\% \times R_{ch\_max}$	**Warning**: R_3 can be optimised by setting its value to R_{ch_max}.
2	$R_3 > R_{ch\_max}$	**Error**: R_3 is set beyond the maximum limit, which may cause load encroachment. It should be set as R_{ch_max}.
3	$R_3 < 90\% \times R_{ch\_max}$	**Error**: R_3 is set too small, failing in providing the maximum fault coverage. It should be set as R_{ch_max}.

Note: R_3 is the zone 3 resistive reach, representing R3 Gnd Res Fwd and R3 Ph Res Fwd; the details on calculation of R_{ch_max} (the ideal resistive reach) is provided in Section B.3.4

Table B.10: Validation rules for R3 Gnd Res Fwd and R3 Ph Res Fwd

When	Then
IN3 Current Set is not equal to 0.1 × I_{max}	**Error**: IN3 Current Set should be set as 10% of the maximum loading current
Note: I_{max} is the maximum loading current	

Table B.11: Validation rule for IN3 Current Set

B.3 Calculation of Associated Variables in the Rules

B.3.1 Calculation of the Line Charging Current I_c

$$\begin{aligned} Z_{base} &= \frac{{V_L}^2}{S_{base}} \\ &= \frac{(400kV)^2}{(100MVA)^2} \\ &= 1600\Omega \end{aligned} \tag{B.1}$$

$$\begin{aligned} I_c &= \frac{V_L}{\sqrt{3} \times \frac{1}{B_1(pu)} \times Z_{base} \times CT_{ratio}} \\ &= \frac{400kV}{\sqrt{3} \times \frac{1}{23.155\%} \times 1600\Omega \times 2000} \\ &= 0.017A \end{aligned} \tag{B.2}$$

where V_L is the line voltage; B_1 is the feeder's positive sequence susceptance; CT_{ratio} is the CT ratio and the calculated I_c is represented in secondary value.

B.3.2 Calculation of the Minimum Fault Current I_{f_min}

The minimum fault current I_{f_min} is calculated under the condition where a 100 Ω resistive Ph-E fault occurs at the remote end with single-end infeed as shown in Figure B.2.

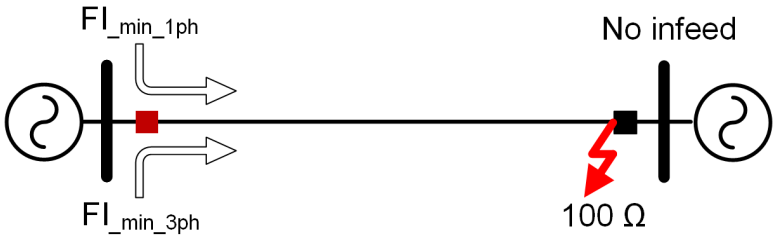


Figure B.2: Single-end infeed with a 100 Ω resistive fault at the remote end

$$\begin{aligned} X_{s1} &= \frac{V_L}{\sqrt{3} \times FI_{\_min\_3ph}} \\ &= \frac{400kV}{\sqrt{3} \times (25.090kA - 8.311kA)} \\ &= 13.764\Omega \\ Z_{s1} &= j13.764\Omega \end{aligned} \tag{B.3}$$

$$\begin{aligned} X_{s0} &= \frac{3 \times V_L/\sqrt{3}}{FI_{\_min\_1ph}} - 2 \times Z_{s1} \\ &= \frac{3 \times 400kV/\sqrt{3}}{21.250kA - 6.233kA} - 2 \times 13.764\Omega \\ &= 18.608\Omega \\ Z_{s0} &= j18.608\Omega \end{aligned} \tag{B.4}$$

$$\begin{aligned} Z_{L1}(\%) &= (0.0727 + j0.795)\% \\ Z_{L1}(\Omega) &= (1.163 + j12.720)\Omega \end{aligned} \tag{B.5}$$

$$\begin{aligned} Z_{L0}(\%) &= (0.354 + j2.098)\% \\ Z_{L0}(\Omega) &= (5.664 + j33.568)\Omega \end{aligned} \tag{B.6}$$

$$
\begin{aligned}
Z_T &= 2 \times (Z_{s1} + Z_{L1}) + Z_{s0} + Z_{L0} + 3 \times R_f \\
&= 2 \times (j13.764 + 1.163 + j12.720) + j18.608 + 5.664 + j33.568 + 3 \times 100 \\
&= 307.990 + j105.144\Omega \\
&= 325.443\angle 18.85^\circ
\end{aligned}
\tag{B.7}
$$

$$
\begin{aligned}
|I_{f\_min}|(primary) &= 3 \times \frac{V_L/\sqrt{3}}{Z_T} \\
&= 3 \times \frac{400kV/\sqrt{3}}{325.443\Omega} \\
&= 2128.853A \\
|I_{f\_min}|(secondary) &= 1.064A
\end{aligned}
\tag{B.8}
$$

where V_L is the line voltage; Z_{s1} is the positive sequence source impedance; Z_{s0} is zero sequence source impedance; Z_{L1} is the positive sequence line impedance; Z_{L0} is zero sequence line impedance; R_f is the fault resistance; FI_{1ph_min} and FI_{3ph_min} are the minimum single-phase and three-phase fault infeeds at the targeted busbar respectively. Z_{s0} is calculated using the series connected positive, negative and zero sequence networks, where details are available in [GSO12].

B.3.3 Sensitivity Check of Differential Protection

The setting of the slopes k_1 and k_2 (as shown in Figure B.3) in differential protection must be configured so that sufficient sensitivity is provided under minimum fault condition, which is defined by the situation where a single-end infeed 100 Ω resistive Ph-E fault occurs at the remote end as specified in Section B.3.2.

Under minimum fault condition,

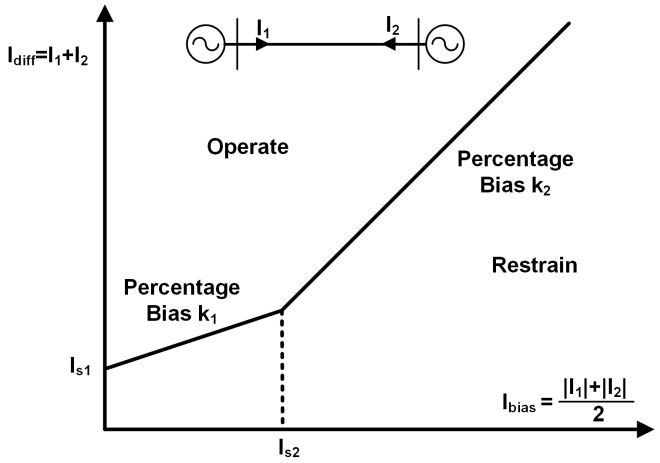


Figure B.3: Biased characteristic of differential protection [Gri11]

$$\begin{aligned} I_{diff} &= I_1 + I_2 \\ &= I_{f\_min} + I_{load} + 0 - I_{load} \\ &= I_{f\_min} \end{aligned} \tag{B.9}$$

$$\begin{aligned} I_{bias} &= \frac{|I_1| + |I_2|}{2} \\ &= \frac{|I_{f\_min} + I_{load}| + |0 + I_{load}|}{2} \\ &= \frac{I_{f\_min} + 2 \times I_{load}}{2} \end{aligned} \tag{B.10}$$

$$I_{op} = \begin{cases} k_1 \times I_{bias} + I_{s1} & I_{bias} < I_{s2} \\ k_1 \times I_{s2} + I_{s1} + k_2 \times (I_{bias} - I_{s2}) & \text{if } I_{bias} \geqslant I_{s2}. \end{cases} \tag{B.11}$$

where I_{diff} is the differential current; I_{bias} is the bias current; I_{load} is the load current and I_{op} is the operating current under certain I_{bias}.

For the sensitivity check, it is required that k_1 and k_2 should be set in such a way that $I_{diff}/I_{op} \geqslant 1.2$. The associated rules are presents in Table B.8 and Table B.9 respectively.

In the shown example in case study 1, $I_{s1} = 0.2$ A, $I_{s2} = 2$ A, $k_1 = 0.5$, and $k_2 = 1.3$.

From Section B.3.2 and the equation B.9, it can be calculated that $I_{diff} = I_{f\_min} = 1.064$ A. It is assumed by the policies that $I_{load} = 1.5$ A (secondary), resulting in $I_{bias} = 2.032$ A (secondary) using equation B.10; based on equation B.11, the current required for the protection to operate is $I_{op} = 1.242$ A. This results in $I_{diff}/I_{op} = 0.857 < 1.2$, therefore violating the rule presented in Table B.8 and Table B.9. In contrast, if $k_1 = 0.3$, and $k_2 = 1.5$ with the same I_{s1} and I_{s2}, following the same calculation procedure, it can be calculated that $I_{diff}/I_{op} = 1.255 > 1.2$, thus conforming to the associated rules.

B.3.4 Calculation of Distance Zone 3 Resistive Reach

In case study 2 reported in Chapter 6, Quad characteristic as shown in Figure B.4 is used. It is required that the resistive reach of distance zone 3 should be set to provide maximum resistive fault coverage while avoiding load encroachment. To achieve this objective, it is required that 20% of load encroachment margin at 30°is provided, which is illustrated in Figure B.4. The optimised zone 3 resistive reach R_{ch_max} can be calculated by:

$$R_{ch\_max} = \frac{V_L}{\sqrt{3} \times \frac{I_{maxload}}{1-20\%}} \times (\cos 30^\circ - \frac{\sin 30^\circ}{\tan RCA}) \tag{B.12}$$

where V_L is the line voltage; $I_{maxload}$ is the maximum loading current (7600 A for 400 kV network); RCA is the relay characteristic angle; and the VT and CT ratios in the actual network are 3600 and 2000 respectively.

In the example in case study 2, RCA = 84°, from which R_{ch_max} can be calculated using equation B.12 as 19.775 Ω (primary)/10.986 Ω (secondary).

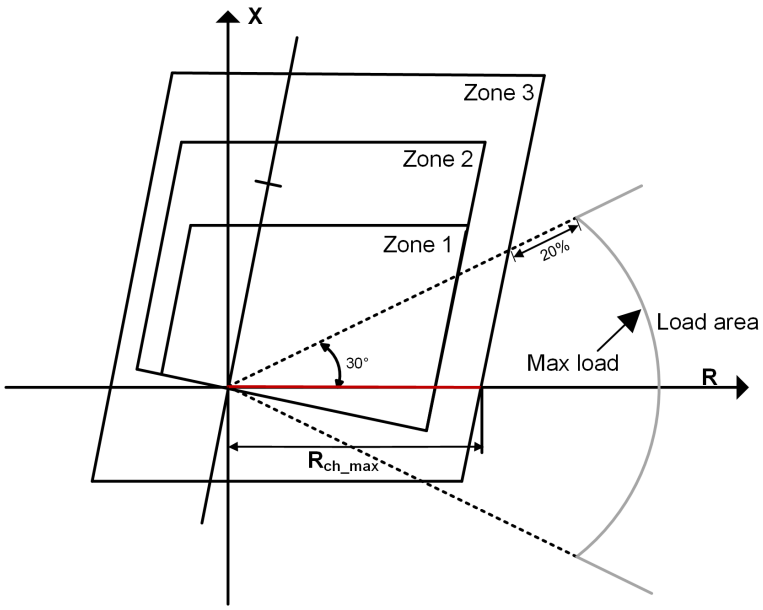


Figure B.4: Setting of zone 3 resistive reach to avoid load encroachment

B.4 Rules for Automated Analysis of MB Simulation Results

This section presents information relating to the criteria used for analysing simulated protection operations in the case studies presented in Chapter 6. In Section B.4.1, rules for analysing the protection operations are presented in a descriptive fashion. In Section B.4.2, where there are many rules involved during the results analysis process, the expected protection elements' behaviours under various validation templates and fault events are presented for ease of understanding. An example of how to represent such expectations in the form of rules is provided.

B.4.1 Rules for Automated Analysis of MB Simulation Results in Case Study 1

When	Then
DIFF_SENS is used; GREN41_min_infeed model is used; I_{DIFF} in IED 1 does not operate	Error. I_{DIFF} should operate under minimum fault condition.
DIFF_SENS is used; SUND42_min_infeed model is used; I_{DIFF} in IED 2 does not operate	Error. I_{DIFF} should operate under minimum fault condition.
DIFF_STAB is used; I_{DIFF} in IED 1 or IED 2 operates	Error. I_{DIFF} should stay stable for maximum external faults.
Note: I_{DIFF} is the differential protection element in IED 1 and IED 2.	

Table B.12: Rules for the analysis of differential protection simulated operations

B.4.2 Rules for Automatic Analysis of MB Simulation Results in Case Study 2

For templates Dist_Loc_Tx and Dist_Rmt_Tx, the expected behaviours of IED 1 are that no elements in the IED should be tripped or activated for any fault events applied.

Element	Expectation
Zone 1 gnd	Should trip for faults within 80% of the line length; should not trip for faults beyond 85% of the line length.
Zone 2 gnd	Should trip for all faults.
Zone 3 gnd	Should trip for all faults.
Zone 4 gnd	Should not be activated for any faults.

Table B.13: Expectations for Dist_Pro_1ph template

Figure B.5 shows the source code of the rule for checking the operation of Zone 1 gnd under the template Dist_Pro_1ph in order to detect incorrect tripping operations during faults located beyond 85% of the line as described in Table B.13.

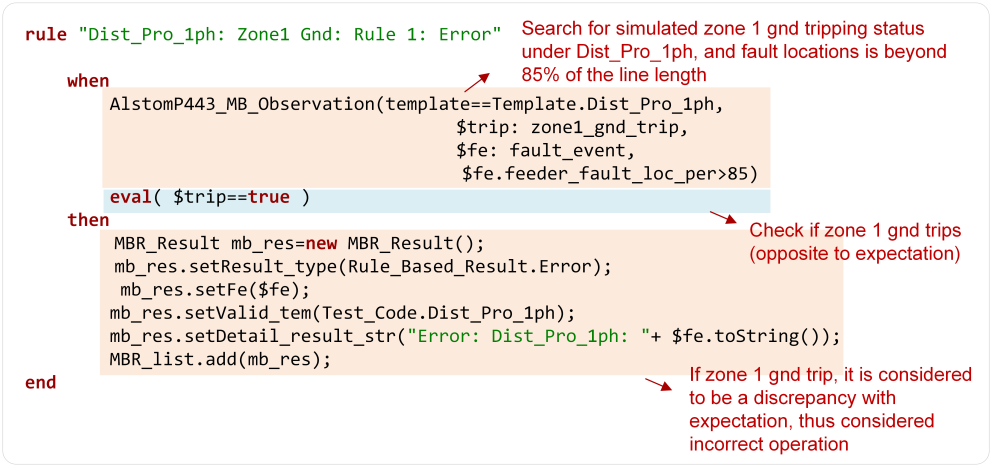


Figure B.5: Source code for checking the incorrect operation of Zone 1 gnd under the template Dist_Pro_1ph

Element	Expectation
Zone 1 ph	Should trip for fault within 80 % of the line length; should not trip for fault beyond 85 % of the line length.
Zone 2 ph	Should trip for all faults.
Zone 3 ph	Should trip for all faults.
Zone 4 ph	Should not be activated for any faults.

Table B.14: Expectations for Dist_Pro_3ph template

Element	Expectation
Zone 1 gnd	Should not trip for any faults.
Zone 2 gnd	Should trip for faults within 25% of the line; should not trip for faults beyond 80% of the line.
Zone 3 gnd	Should trip for all faults.
Zone 4 gnd	Should not be activated for any faults.

Table B.15: Expectations for Dist_F1_1ph template

Element	Expectation
Zone 1 ph	Should not trip for any faults.
Zone 2 ph	Should trip for faults within 25% of the line; should not trip for faults beyond 80% of the line.
Zone 3 ph	Should trip for all faults.
Zone 4 ph	Should not be activated any all faults.

Table B.16: Expectations for Dist_F1_3ph template

Element	Expectation
Zone 1 gnd	Should not trip for any faults.
Zone 2 gnd	Should not trip for any faults.
Zone 3 gnd	Should not trip for any faults.
Zone 4 gnd	Should be activated as long as Zone 2 gnd in the relay at remote end trips; should not be activated for faults beyond 85% of the R1 branches.

Table B.17: Expectations for Dist_R1_1ph template

Element	Expectation
Zone 1 ph	Should not trip for any faults.
Zone 2 ph	Should not trip for any faults.
Zone 3 ph	Should not trip for any faults.
Zone 4 ph	Should be activated as long as Zone 2 ph in the relay at remote end trips; should not be activated for faults beyond 85% of the R1 branches.

Table B.18: Expectations for Dist_R1_3ph template

Bibliography

[A. 13a] A. Apostolov. Disturbance analysis for the 21st century. *Pacworld Magazine*, page 4, June 2013. (cited on pages 69, 81)

[A. 13b] A. Apostolov. Event and disturbance analysis - common data formats. *Pacworld Magazine*, pages 47–51, Jun 2013. (cited on pages 5, 69, 81)

[A. 14] A. Wen, M. Zhao, J. Li et al. On-line evaluation and verification of protection relay settings - design and field experience. In *Developments in Power System Protection (DPSP 2014), 12th IET International Conference on*, pages 1–4, March 2014. doi:10.1049/cp.2014.0004. (cited on pages 3, 38, 49)

[AADK+03] H. Abyaneh, M. Al-Dabbagh, H. Karegar, S. Sadeghi, and R. Khan. A new optimal approach for coordination of overcurrent relays in interconnected power systems. *Power Delivery, IEEE Transactions on*, 18(2):430–435, April 2003. doi:10.1109/TPWRD.2002.803754. (cited on page 32)

[ABB12] ABB. Line distance protection REL670 Technical reference manual, 2012. (cited on pages 67, 74, 86, 126)

[ABB14] ABB. Line differential protection RED670 2.0 IEC Technical Manual, 2014. (cited on page 126)

[ADB14] I. Abdulhadi, A. Dysko, and G. Burt. Reachability analysis for the verification of adaptive protection setting selection logic. *Power Delivery, IEEE Transactions on*, 29(5):2206–2214, Oct 2014. doi:10.1109/TPWRD.2014.2304614. (cited on page 36)

[Alp10] E. Alpaydn. *Introduction to Machine Learning*. The MIT Press, 2010. (cited on page 57)

[Als11a] Alstom Grid. MiCOM P543, P544, P545, P546 Technical Manual, 2011. (cited on pages xi, 67, 74, 126, 129, 130)

[Als11b] Alstom Grid. MiCOMho P443, P445 Technical Manual, 2011. (cited on pages xii, 24, 67, 74, 76, 78, 86, 104, 126, 140, 142)

[AP94] A. Aamodt and E. Plaza. Case-based reasoning: Foundational issues, methodological variations, and system approaches. *AI Communications*, 7(1):39–59, 1994. (cited on pages vii, 54)

[Apo05] A. Apostolov. Simplifying the configuration of multifunctional distribution protection and control IEDs. In *Electricity Distribution, 2005. CIRED 2005. 18th International Conference and Exhibition on*, pages 1–4, June 2005. (cited on pages 6, 70)

[AS97] R. Aggarwal and Y. Song. Artificial neural networks in power systems I: General introduction to neural computing. *Power Engineering Journal*, 11(3):129–134, June 1997. doi:10.1049/pe:19970306. (cited on page 57)

[AS09] A. Atputharajah and T. Saha. Power system blackouts - literature review. In *Industrial and Information Systems (ICIIS), 2009 International Conference on*, pages 460–465, Dec 2009. doi:10.1109/ICIINFS.2009.5429818. (cited on pages 1, 1)

[AV07] A. Apostolov and B. Vandiver. On the standardisation of distance characteristics. In *Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources, 2007. PSC 2007*, pages 209–212, March 2007. doi:10.1109/PSAMP.2007.4740913. (cited on pages 5, 69, 81)

[BCBB13] S. Blair, F. Coffele, C. Booth, and G. Burt. An open platform for rapid-prototyping protection and control schemes with IEC 61850. *Power Delivery, IEEE Transactions on*, 28(2):1103–1110, April 2013. doi:10.1109/TPWRD.2012.2231099. (cited on pages 73, 77, 88)

[BDF+93] A. Beschta, O. Dressler, H. Freitag, M. Montag, and P. Struss. A model-based approach to fault localisation in power transmission networks. *Intelligent Systems Engineering*, 2(1):3–14, Spring 1993. (cited on page 49)

[BGK+14] T. Bopp, R. Ganjavi, R. Krebs, B. Ntsin, M. Dauer, and J. Jaeger. Improving grid reliability through application of protection security assessment. In *Developments in Power System Protection (DPSP 2014), 12th IET International Conference on*, pages 1–5, March 2014. doi:10.1049/cp.2014.0009. (cited on page 3)

[Bla13] S. Blair. *The Analysis and Application of Resistive Superconducting Fault Current Limiters in Present and Future Power Systems*. PhD thesis, University of Strathclyde, 2013. (cited on pages vii, 15, 22)

[BMM+98] S. Bell, S. McArthur, J. McDonald, G. Burt, R. Mather, and T. Cumming. Model-based analysis of protection system performance. *Generation, Transmission and Distribution, IEE Proceedings*, 145(5):547–552, Sep 1998. doi:10.1049/ip-gtd:19982183. (cited on page 49)

[Bra01] I. Bratko. *Prolog Programming for Artificial Intelligence: programming for artificial intelligence*. Pearson Education, 2001. (cited on page 44)

[BS88] V. Bapeswara and K. Sankara. Computer aided coordination of directional relays: determination of break points. *Power Delivery, IEEE Transactions on*, 3(2):545–548, Apr 1988. doi:10.1109/61.4291. (cited on page 32)

[BS14] M. Bianchini and F. Scarselli. On the complexity of neural network classifiers: A comparison between shallow and deep architectures. *Neural Networks and Learning Systems, IEEE Transactions on*, 25(8):1553–1565, Aug 2014. doi:10.1109/TNNLS.2013.2293637. (cited on page 58)

[BTRS94] R. Broadwater, J. Thompson, S. Rahman, and A. Sargent. An expert system for integrated protection design with configurable distribution

circuits. *Power Delivery, IEEE Transactions on*, 9(2):1115–1121, Apr 1994. doi:10.1109/61.296297. (cited on page 46)

[Bur12] N. Burnham. Network Rail and IEC 61850, a user's perspective of the standard. In *Developments in Power Systems Protection, 2012. DPSP 2012. 11th International Conference on*, pages 1–5, April 2012. doi:10.1049/cp.2012.0016. (cited on pages 6, 70, 82)

[But01] S. Butler. UK electricity networks - the nature of UK electricity transmission and distribution networks in an intermittent renewable and embedded electricity generation future, 2001. URL: http://www.parliament.uk/documents/post/e5.pdf. (cited on pages vii, 13)

[CBB+13] F. Coffele, S. Blair, C. Booth, J. Kirkwood, and B. Fordyce. Demonstration of adaptive overcurrent protection using IEC 61850 communications. In *Electricity Distribution (CIRED 2013), 22nd International Conference and Exhibition on*, pages 1–4, June 2013. doi:10.1049/cp.2013.0646. (cited on pages 5, 69, 81)

[CBD15] F. Coffele, C. Booth, and A. Dysko. An adaptive overcurrent protection scheme for distribution networks. *Power Delivery, IEEE Transactions on*, 30(2):561–568, April 2015. doi:10.1109/TPWRD.2013.2294879. (cited on page 36)

[CIG13] CIGRE Working Group B5.31. Life-time management of relay settings. Technical report, CIGRE, 2013. (cited on pages vii, 28, 29, 68)

[CIG14] CIGRE Working Group B5.27. Implications and benefits of standardised protection and control schemes. Technical report, CIGRE, 2014. (cited on page 68)

[CJ98] D. Coury and D. Jorge. Artificial neural network approach to distance protection of transmission lines. *Power Delivery, IEEE Transactions on*, 13(1):102–108, Jan 1998. doi:10.1109/61.660861. (cited on pages 59, 60)

[CS15] V. Catterson and B. Sheng. Deep neural networks for understanding and diagnosing partial discharge data. In *Electrical Insulation Conference (EIC), 2015 IEEE*, pages 1–6, June 2015. (cited on page 58)

[CSS96] B. Chattopadhyay, M. Sachdev, and T. Sidhu. An on-line relay coordination algorithm for adaptive protection using linear programming technique. *Power Delivery, IEEE Transactions on*, 11(1):165–173, Jan 1996. doi:10.1109/61.484013. (cited on page 32)

[DIg11a] DIgSILENT PowerFactory. DIgSILENT PowerFactory 15 user manual, 2011. (cited on pages 38, 49, 94)

[DIg11b] DIgSILENT PowerFactory. DIgSILENT technical documentation PowerFactory API, 2011. (cited on page 120)

[DMM03] E. Davidson, S. McArthur, and J. McDonald. A toolset for applying model-based reasoning techniques to diagnostics for power systems protection. *Power Systems, IEEE Transactions on*, 18(2):680–687, May 2003. doi:10.1109/TPWRS.2003.810981. (cited on pages vii, 48, 49, 81, 119)

[DRVP84] M. Damborg, R. Ramaswami, S. Venkata, and J. Postforoosh. Computer aided transmission protection system design part i: algorithms. *Power Apparatus and Systems, IEEE Transactions on*, PAS-103(1):51–59, Jan 1984. doi:10.1109/TPAS.1984.318576. (cited on page 32)

[DV84] M. Damborg and S. Venkata. *Specification of computer-Aided design of transmission protection systems*. EPRI, 1984. (cited on page 33)

[E3 10] E3 - Spanish Electricity Companies for Studies on IEC 61850. Minimum common specification for substation protection and control equipment in accordance with the IEC 61850 standard, June 2010. (cited on pages 6, 70)

[EAJMB05] K. El-Arroudi, G. Joos, D. McGillis, and R. Brearley. Comprehensive transmission distance protection settings using an intelligent-based

analysis of events and consequences. *Power Delivery, IEEE Transactions on*, 20(3):1817–1824, July 2005. doi:10.1109/TPWRD.2005.848656. (cited on pages 3, 31, 34, 46)

[Ecl14a] Eclipse Foundation. Eclipse, 2014. URL: https://eclipse.org/. (cited on page 99)

[Ecl14b] Eclipse Foundation. Eclipse Modeling - EMF - Home, 2014. URL: http://www.eclipse.org/modeling/emf/. (cited on pages 73, 77)

[EDM+13] C. Edwards, E. Davidson, S. McArthur, I. Watt, and T. Cumming. Flexible model-based alarm processing for protection performance assessment and incident identification. *Power Systems, IEEE Transactions on*, 28(3):2584–2591, Aug 2013. doi:10.1109/TPWRS.2013.2243763. (cited on page 49)

[Ele15] Electrocon International Inc. CAPE Software, 2015. URL: http://www.electrocon.com/index.php. (cited on pages 3, 38, 49)

[ENT12] ENTSO-E. ENTSO-E statement on the IEC 61850 standard, 2012. (cited on pages 6, 70)

[ETA15] ETAP. ETAP, 2015. URL: http://etap.com/. (cited on pages 3, 38, 49)

[FK86] C. Fukui and J. Kawakami. An expert system for fault section estimation using information from protective relays and circuit breakers. *Power Delivery, IEEE Transactions on*, 1(4):83–90, Oct 1986. doi:10.1109/TPWRD.1986.4308033. (cited on page 46)

[FTKM12] A. Filippo, Jr. A. Torres, B. Kjerfve, and A. Monat. Application of artificial neural network (ANN) to improve forecasting of sea level. *Ocean and Coastal Management*, 55(0):101–110, 2012. URL: http://www.sciencedirect.com/science/article/pii/S0964569111001475, doi:http://dx.doi.org/10.1016/j.ocecoaman.2011.09.007. (cited on page 58)

[G. 14] G. Huon, A. Apostolov, R. Paulo et al. IEC 61850 based substation automation systems users expectations and stakeholders interactions. In *CIGRE Paris Session*, 2014. (cited on pages 6, 68, 70)

[GB10] X. Glorot and Y. Bengio. Understanding the difficulty of training deep feedforward neural networks. In *13th International Conference on Artificial Intelligence and Statistics (AISTATS)*, pages 1–6, 2010. (cited on page 58)

[GE 12a] GE Digital Energy. D60 line distance protection system UR series instruction manual, 2012. (cited on pages 67, 74, 86, 126)

[GE 12b] GE Digital Energy. D90 plus line distance protection system instruction manual, 2012. (cited on page 126)

[Gri11] Alstom Grid. *Network protection & automation guide*. Alstom Grid, 2011. (cited on pages vii, x, 16, 17, 18, 20, 23, 25, 26, 27, 37, 86, 181)

[GSO12] J. Glover, M. Sarma, and T. Overbye. *Power System Analysis and Design*. Cengage Learning, 2012. (cited on pages 12, 162, 168, 180)

[HBC+13] Q. Hong, S. Blair, V. Catterson, A. Dysko, C. Booth, and T. Rahman. Standardisation of power system protection settings using IEC 61850 for improved interoperability. In *Power and Energy Society General Meeting (PES), 2013 IEEE*, pages 1–5, July 2013. doi:10.1109/PESMG.2013.6672816. (cited on pages 5, 66, 69, 74)

[HDB12] Q. Hong, A. Dysko, and C. Booth. Intelligent system for detecting hidden errors in protection settings. In *Universities Power Engineering Conference (UPEC), 2012 47th International*, pages 1–6, Sept 2012. doi:10.1109/UPEC.2012.6398575. (cited on pages 5, 98)

[HVNS08] N. Higgins, V. Vyatkin, N. Nair, and K. Schwarz. Concept for intelligent distributed power system automation with IEC 61850 and IEC 61499. In *Systems, Man and Cybernetics, 2008. SMC 2008. IEEE International Conference on*, pages 36–41, Oct 2008. doi:10.1109/ICSMC.2008.4811247. (cited on page 72)

[IEC01] IEC. IEC 60909-0: short-circuit currents in three-phase systems: part 0: calculation of currents, 2001. (cited on page 14)

[IEC03] IEC TC 57. IEC 61850-1: Introduction and overview, 2003. (cited on pages viii, 69, 73, 77, 83)

[IEC09] IEC. IEC 60255-151: measuring relays and protection equipment: part 151: functional requirements for over/under current protection, 2009. (cited on page 26)

[IEC10a] IEC TC 57. IEC 61850-6: configuration description language for communication in electrical substations related to IEDs, 2010. (cited on pages 4, 66, 70, 72)

[IEC10b] IEC TC 57. IEC 61850-7-3: basic communication structure - common data classes, 2010. (cited on page 70)

[IEC10c] IEC TC 57. IEC 61850 7-4: basic communication structure - compatible logical node classes and data object classes, 2010. (cited on page 70)

[IEE06] IEEE. IEEE recommended practice for excitation system models for power system stability studies. *IEEE Std 421.5-2005 (Revision of IEEE Std 421.5-1992)*, 2006. doi:10.1109/IEEESTD.2006.99499. (cited on page 12)

[IEE13] IEEE Power System Relaying Committee Working Group H5. Common format for IED configuration data. Technical report, IEEE, 2013. (cited on pages 67, 69, 71)

[IEE14] IEEE Power System Relaying Committee Working Group H27. Power System Relaying Committee Working Group H27 Common Format for Relay Settings Data, 2014. URL: http://www.pes-psrc.org/h/h27/h27.html. (cited on page 68)

[JBRRGM14] M. Jaya Bharata Reddy, D. Rajesh, P. Gopakumar, and D. Mohanta. Smart fault location for smart grid operation using RTUs and computational intelligence techniques. *Systems Journal, IEEE*, 8(4):1260–1271, Dec 2014. doi:10.1109/JSYST.2014.2303833. (cited on page 59)

[JKSD92] L. Jenkins, H. Khincha, S. Shivakumar, and P. Dash. An application of functional dependencies to the topological analysis of protection schemes. *Power Delivery, IEEE Transactions on*, 7(1):77–83, Jan 1992. doi:10.1109/61.108892. (cited on page 32)

[KEDH02] M. Kandil, S. El-Debeiky, and N. Hasanien. Long-term load forecasting for fast developing utility using a knowledge-based expert system. *Power Systems, IEEE Transactions on*, 17(2):491–496, May 2002. doi:10.1109/TPWRS.2002.1007923. (cited on page 46)

[KNUF92] T. Kimura, S. Nishimatsu, Y. Ueki, and Y. Fukuyama. Development of an expert system for estimating fault section in control center based on protective system simulation. *Power Delivery, IEEE Transactions on*, 7(1):167–172, Jan 1992. doi:10.1109/61.108904. (cited on page 46)

[KSK+93] K. Kawahara, H. Sasaki, J. Kubokawa, H. Sugihara, and M. Kitagawa. An expert system for supporting protective relay setting for transmission lines. In *Developments in Power System Protection, 1993., Fifth International Conference on*, pages 203–206, 1993. (cited on pages 3, 34, 46)

[KSS97] K. Kawahara, H. Sasaki, and H. Sugihara. An application of rule based system to the coordination of directional overcurrent relays. In *Developments in Power System Protection, Sixth International Conference on (Conf. Publ. No. 434)*, pages 58–61, Mar 1997. doi:10.1049/cp:19970028. (cited on pages 3, 34, 46)

[KV91] D. Kirschen and T. Volkmann. Guiding a power system restoration with an expert system. *Power Systems, IEEE Transactions on*, 6(2):558–566, May 1991. doi:10.1109/59.76698. (cited on pages 4, 46)

[KW87] J. Kleer and B. Williams. Diagnosing Multiple Faults, 1987. URL: http://groups.csail.mit.edu/mers/papers/kle-wil-92.pdf. (cited on page 49)

[LCAY01] S. Lee, M. Choi, B. Ahn, and N. Yoon. A new efficient setting method for protective devices in distribution systems using heuristic rules. In

Power Engineering Society Summer Meeting, 2001, volume 2, pages 1193–1198 vol.2, 2001. doi:10.1109/PESS.2001.970234. (cited on page 33)

[LFST94] R. Leitch, H. Freitag, A. Stefanini, and G. Tornielli. Using the artist approach for diagnosing power transmission networks. *Intelligent Systems Engineering*, 3(3):125–137, Autumn 1994. (cited on page 49)

[LL96] S. Lee and C. Liu. Intelligent approach to coordination identification in distance relaying. In *Intelligent Systems Applications to Power Systems, 1996. Proceedings, ISAP 1996., International Conference on*, pages 62–67, Jan 1996. doi:10.1109/ISAP.1996.501045. (cited on pages 3, 33, 46)

[Lug09] G. Luger. *Artificial intelligence : structures and strategies for complex problem solving*. Pearson Education, 2009. (cited on pages vii, 41, 42, 43, 44, 45, 47, 48, 53, 54, 56, 58, 63, 98)

[LYYJ90] S. Lee, S. Yoon, M. Yoon, and J. Jang. An expert system for protective relay setting of transmission systems. *Power Delivery, IEEE Transactions on*, 5(2):1202–1208, Apr 1990. doi:10.1109/61.53142. (cited on pages 3, 32, 33, 46)

[M. 94] M. Enns, L. Budler, T. Cease et al. Potential applications of expert systems to power system protection. *Power Delivery, IEEE Transactions on*, 9(2):720–728, Apr 1994. doi:10.1109/61.296249. (cited on pages 42, 45, 46)

[Mac08] D. MacKay. *Sustainable Energy - without the hot air*. UIT Cambridge Ltd., 2008. (cited on page 2)

[MAE+04] A. McMorran, G. AuIt, I. Elders, C. Foote, G. Burt, and J. McDonald. Translating CIM XML power system data to a proprietary format for system simulation. In *Power Engineering Society General Meeting, 2004. IEEE*, pages 116 Vol.1–, June 2004. doi:10.1109/PES.2004.1372768. (cited on page 78)

[MAM+06] A. McMorran, G. Ault, C. Morgan, I. Elders, and J. Mcdonald. A common information model (CIM) toolkit framework implemented in Java. *Power Systems, IEEE Transactions on*, 21(1):194–201, Feb 2006. doi:10.1109/TPWRS.2005.857846. (cited on page 69)

[MBL+98] J. Mahseredjian, G. Benmouyal, X. Lombard, M. Zouiti, B. Bressac, and L. Gerin-Lajoie. A link between EMTP and MATLAB for user-defined modeling. *Power Delivery, IEEE Transactions on*, 13(2):667–674, Apr 1998. doi:10.1109/61.660959. (cited on page 119)

[McA96] S. McArthur. *Knowledge and Model Based Reasoning for Power System Protection Performance Analysis*. PhD thesis, University of Strathclyde, 1996. (cited on pages 44, 54)

[MDC+07] S. McArthur, E. Davidson, V. Catterson, A. Dimeas, N. Hatziargyriou, F. Ponci, and T. Funabashi. Multi-agent systems for power engineering applications-part i: concepts, approaches, and technical challenges. *Power Systems, IEEE Transactions on*, 22(4):1743–1752, Nov 2007. doi:10.1109/TPWRS.2007.908471. (cited on page 42)

[MDDM03] S. McArthur, E. Davidson, G. Dudgeon, and J. McDonald. Toward a model integration methodology for advanced applications in power engineering. *Power Systems, IEEE Transactions on*, 18(3):1205–1206, Aug 2003. doi:10.1109/TPWRS.2003.814908. (cited on pages 47, 49)

[MDM+96] S. McArthur, A. Dysko, J. McDonald, S. Bell, R. Mather, and S. Burt. The application of model based reasoning within a decision support system for protection engineers. *Power Delivery, IEEE Transactions on*, 11(4):1748–1754, Oct 1996. doi:10.1109/61.544253. (cited on pages 4, 46, 49)

[MIK+95] T. Minakawa, Y. Ichikawa, M. Kunugi, K. Shimada, N. Wada, and M. Utsunomiya. Development and implementation of a power system fault diagnosis expert system. *Power Systems, IEEE Transactions on*, 10(2):932–940, May 1995. doi:10.1109/59.387936. (cited on page 46)

[Mit97] T. Mitchell. *Machine Learning.* McGraw-Hill Science/Engineering/Math, 1997. (cited on pages vii, 56, 57, 58, 59)

[Nat03] National Grid. Investigation report into the loss of supply incident affecting parts of south London at 18:20 on Thursday, 28 August 2003, 2003. URL: `http://www.g4jnt.com/hams_hall_investigation_report.pdf`. (cited on pages 2, 140)

[Nat14] National Grid. Electricity Ten Year Statement 2014, 2014. URL: `http://www2.nationalgrid.com/UK/Industry-information/Future-of-Energy/Electricity-Ten-Year-Statement/`. (cited on pages 14, 161)

[OGH03] E. Orduna, F. Garces, and E. Handschin. Algorithmic-knowledge-based adaptive coordination in transmission protection. *Power Delivery, IEEE Transactions on*, 18(1):61–65, Jan 2003. `doi:10.1109/TPWRD.2002.806683`. (cited on page 36)

[Omi11] Omicron. XRIO user manual, 2011. (cited on page 72)

[Ora14] Oracle. Java, 2014. URL: `http://java.com/en/`. (cited on pages 73, 94)

[PL97] Y. Park and K. Lee. Application of expert system to power system restoration in sub-control center. *Power Systems, IEEE Transactions on*, 12(2):629–635, May 1997. `doi:10.1109/59.589628`. (cited on pages 4, 46)

[PPS91] V. Prasad, K. Prakaso, and A. Subba. Coordination of directional relays without generating all circuits. *Power Delivery, IEEE Transactions on*, 6(2):584–590, Apr 1991. `doi:10.1109/61.131115`. (cited on page 32)

[PU01] L. Perez and A. Urdaneta. Optimal computation of distance relays second zone timing in a mixed protection scheme with directional overcurrent relays. *Power Delivery, IEEE Transactions on*, 16(3):385–388, Jul 2001. `doi:10.1109/61.924815`. (cited on page 32)

[PW03] B. Peischl and F. Wotawa. Model-based diagnosis or reasoning from first principles. *Intelligent Systems, IEEE*, 18(3):32–37, May 2003. doi:10.1109/MIS.2003.1200725. (cited on page 47)

[PWN92] M. Pfau-Wagenbauer and W. Nejdl. Integrating model-based and heuristic features in a real-time expert system for power distribution networks. In *Artificial Intelligence for Applications, 1992., Proceedings of the Eighth Conference on*, pages 303–309, Mar 1992. doi:10.1109/CAIA.1992.200046. (cited on pages 4, 46)

[R. 77] R. Gastineau, R. Harris, Jr. W. Woodside, and W. Scribner. Using the computer to set transmission line phase distance and ground back-up relays. *Power Apparatus and Systems, IEEE Transactions on*, 96(2):478–484, Mar 1977. doi:10.1109/T-PAS.1977.32357. (cited on page 32)

[RBM01] M. Redfern, Z. Bo, and D. Montjean. Detection of broken conductors using the positional protection technique. In *Power Engineering Society Summer Meeting, 2001*, volume 2, pages 1163–1168 vol.2, 2001. doi:10.1109/PESS.2001.970229. (cited on page 12)

[Red13] Red Hat Inc. JBoss Enterprise BRMS Platform 5 JBoss Rules 5 Reference Guide, 2013. (cited on pages 44, 98, 100)

[RMJ10] S. Rudd, S. Mcarthur, and M. Judd. A generic knowledge-based approach to the analysis of partial discharge data. *Dielectrics and Electrical Insulation, IEEE Transactions on*, 17(1):149–156, February 2010. doi:10.1109/TDEI.2010.5412013. (cited on pages 44, 46)

[RN10] S. Russell and P. Norvig. *Artificial intelligence - a modern approach*. Pearson Education, 2010. (cited on pages 41, 42, 57)

[Rud10] S. Rudd. *Knowledge-Based Analysis of Partial Discharge Data*. PhD thesis, University of Strathclyde, 2010. (cited on pages 44, 101)

[RVDP84] R. Ramaswami, S. Venkata, M. Damborg, and J. Postforoosh. Computer aided transmission protection system design part ii: implementation and results. *Power Apparatus and Systems, IEEE Transactions on*,

PAS-103(1):60–65, Jan 1984. doi:10.1109/TPAS.1984.318577. (cited on page 32)

[SAA+00] G. Schreiber, H. Akkermans, A. Anjewierdn, R. Hogg, N. Shadbolt, W. Velde, and B. Wielinga. *Knowledge engineering and management, the CommonKADS methodology.* The MIT Press, 2000. (cited on page 101)

[SBG02] E. Styvaktakis, M. Bollen, and I. Gu. Expert system for classification and analysis of power system events. *Power Delivery, IEEE Transactions on*, 17(2):423–428, Apr 2002. doi:10.1109/61.997911. (cited on pages 4, 46)

[Sie00] Siemens. SIPROTEC 7SD522 distance protection manual, 2000. (cited on page 126)

[Sie11a] Siemens. Global blackouts - lessons learned, 2011. (cited on page 1)

[Sie11b] Siemens. SIPROTEC: line differential protection with distance protection 7SD5 manual, 2011. (cited on page 126)

[Sie13] Siemens. SIPROTEC 5 IEC 61850 manual, 2013. (cited on page 67)

[Sie15] Siemens. SIGUARD PSA: Protection Security Assessment, 2015. URL: http://w3.siemens.com/smartgrid/global/en/products-systems-solutions/control-center-solutions/siguard/pages/siguard-psa.aspx. (cited on pages 38, 49)

[SKS+00] E. Senger, W. Kaiser, J. Santos, P. Burt, and C. Malagodi. Broken conductors protection system using carrier communication. *Power Delivery, IEEE Transactions on*, 15(2):525–530, Apr 2000. doi:10.1109/61.852979. (cited on page 12)

[SL00] C. So and K. Li. Time coordination method for power system protection by evolutionary algorithm. *Industry Applications, IEEE Transactions on*, 36(5):1235–1240, Sep 2000. doi:10.1109/28.871269. (cited on pages 3, 35, 59, 81)

[Slu97] L. Sluis. Adaptive distance protection of double-circuit lines using artificial neural networks. *Power Delivery, IEEE Transactions on*, 12(1):97–105, Jan 1997. doi:10.1109/61.568229. (cited on page 59)

[SMB+10] J. Sykes, V. Madani, J. Burger, M. Adamiak, and W. Premerlani. Reliabilty of protection systems (what are the real concerns). In *Protective Relay Engineers, 2010 63rd Annual Conference for*, pages 1–16, March 2010. doi:10.1109/CPRE.2010.5469482. (cited on pages 2, 5, 6, 18, 19, 30, 69, 70, 82)

[SWH94] G. Schreiber, B. Wielinga, and R. Hogg. CommonKADS: a comprehensive methodology for KBS development. *IEEE Expert*, pages 28–37, 1994. (cited on page 101)

[SWI15] SWIG. SWIG, 2015. URL: http://www.swig.org/. (cited on page 120)

[SWM+01] S. Strachan, G. West, J. McDonald, A. Duffy, J. Farrell, and B. Gwyn. Knowledge management and intelligent decision support for protection scheme design and application in electrical power systems. In *Developments in Power System Protection, 2001, Seventh International Conference on (IEE)*, pages 559–562, 2001. doi:10.1049/cp:20010223. (cited on page 55)

[TBRS94] J. Thompson, R. Broadwater, S. Rahman, and A. Sargent. An expert system for integrated protection design with configurable distribution circuits: II. *Power Delivery, IEEE Transactions on*, 9(2):1122–1128, Apr 1994. doi:10.1109/61.296298. (cited on page 46)

[TCK+00] J. Tan, P. Crossley, D. Kirschen, J. Goody, and J. Downes. An expert system for the back-up protection of a transmission network. *Power Delivery, IEEE Transactions on*, 15(2):508–514, Apr 2000. doi:10.1109/61.852976. (cited on page 46)

[TCM+02] J. Tan, P. Crossley, P. McLaren, P. Gale, I. Hall, and J. Farrell. Application of a wide area backup protection expert system to prevent

cascading outages. *Power Delivery, IEEE Transactions on*, 17(2):375–380, Apr 2002. doi:10.1109/61.997902. (cited on page 46)

[Tsi64] H. Tsien. An automatic digital computer program for setting transmission line directional overcurrent relays. *Power Apparatus and Systems, IEEE Transactions on*, 83(10):1048–1053, Oct 1964. doi:10.1109/TPAS.1964.4765939. (cited on page 32)

[Uni04] Union of the Electricity Industry. Power outages in 2003, 2004. (cited on pages 1, 2)

[UPR97] A. Urdaneta, L. Perez, and H. Restrepo. Optimal coordination of directional overcurrent relays considering dynamic changes in the network topology. *Power Delivery, IEEE Transactions on*, 12(4):1458–1464, Oct 1997. doi:10.1109/61.634161. (cited on page 32)

[VRF+99] Z. Vale, C. Ramos, L. Faria, N. Malheiro, A. Silva, and A. Marques. SPARSE-an intelligent alarm processor for Portuguese transmission control centres. In *Human Interfaces in Control Rooms, Cockpits and Command Centres, 1999. International Conference on*, pages 446–451, Jun 1999. doi:10.1049/cp:19990231. (cited on pages 4, 46)

[W3C14] W3C. XML Schema, 2014. URL: http://www.w3.org/XML/Schema. (cited on pages 73, 77)

[Wor07] World Energy Council. Deciding the future: energy policy scenarios to 2050. Technical report, 2007. (cited on page 2)

[WSM+01a] G. West, S. Strachan, J. McDonald, A. Duffy, J. Farrell, and B. Gwyn. DEKAS - an evolutionary case-based reasoning system to support protection scheme design. 2001. IMechE Professional Engineering Publishing, pp123-130. (cited on page 55)

[WSM+01b] G. West, S. Strachan, A. Moyes, J. McDonald, B. Gwyn, and J. Farrell. Knowledge management and decision support for electrical power utilities. *Knowledge and Process Management*, 8(4):207–216, 2001. doi:10.1002/kpm.124. (cited on page 55)

[WSMM01] G. West, S. Strachan, A. Moyes, and J. McDonald. Intelligent engineering support for protection scheme design. In *Power Engineering, 2001. LESCOPE '01. 2001 Large Engineering Systems Conference on*, pages 54–58, 2001. doi:10.1109/LESCPE.2001.941626. (cited on page 55)

[X. 14a] X. Zhao, L. Li, and G. Huon. CIGRE 2014 Group 5 (Protection and Automation) discussion meeting summary (2014 CIGRE Paris Session), August 2014. (cited on pages 6, 70)

[X. 14b] X. Zhao, L. Li, and G. Huon. CIGRE 2014 special report for SC B5, August 2014. (cited on page 82)

[XLD94] Y. Xia, K. Li, and A. David. Adaptive relay setting for stand-alone digital distance protection. *Power Delivery, IEEE Transactions on*, 9(1):480–491, Jan 1994. doi:10.1109/61.277720. (cited on pages 36, 37)

[Xu94] L. Xu. Case based reasoning. *Potentials, IEEE*, 13(5):10–13, Dec 1994. doi:10.1109/45.464654. (cited on pages 53, 54)

[Y. 13] Y. Paithankar and S. Bhide. *Fundamentals of power system protection.* PHI Learning Private Limited, 2013. (cited on pages vii, xi, 12, 13, 14)