University of Southern Queensland
Faculty of Health, Engineering and Sciences

Remote Management of Safety Systems in Power Utility Installations

A dissertation submitted by

Paul Hohenhaus

In fulfilment of the requirements of

ENG4111/ENG4112 Research Project

Towards the degree of

Bachelor of Engineering (Power)

Submitted: October 2015

Abstract

Within the power industry protection schemes that are designed to protect electrical plant and the public from power system events can be described as safety related systems. Power utilities are under increasing pressure to provide a cost effective, reliable and safe power network. To accommodate these expectations efficiencies in existing infrastructure and operating techniques warrant continual examination. Infrastructure providing remote connectivity to IEDs already exists, however the changing of protection functions remotely has been avoided over concerns of a change in verification methods. Owing to the number installed and the geographic diversity a request for a remote change will be inevitable.

To respond to these requests, the project examined three key areas which were deemed crucial to the success of remote delivery of Protection IED configuration files;

- Development of configuration files are consistently free of error
- Development of a robust alternate verification method that supports remote configuration delivery and is comparable against traditional methods
- Understanding the Protection IED's responds to a configuration delivery whilst remaining in service; and the operational risk that it may be impose.

These were collectively examined and addressed by the prescribed objectives outlined in the project. Through assessment of an existing configuration delivery workflow, targeted checklists were developed and assessed to provide an improved workflow output reducing the probability of error in configuration development. Deficiencies highlighted in internal case study assisted with the development of an alternate verification process, which was assessed against prescribed legislative and regulatory requirements imposed on Distribution Network Service providers; with a further assessment undertaken against Ergon Energy's traditional methods for configuration delivery.

The outcomes of the project were able to describe and evaluate the systems, processes and criteria needed to facilitate remote management of selected protection IEDs installed on Ergon Energy's distribution network.

Limitations of Use

University of Southern Queensland

Faculty of Health, Engineering and Sciences

ENG4111/ENG4112 Research Project

Limitations of Use

The Council of the University of Southern Queensland, its Faculty of Health, Engineering & Sciences, and the staff of the University of Southern Queensland, do not accept any responsibility for the truth, accuracy or completeness of material contained within or associated with this dissertation.

Persons using all or any part of this material do so at their own risk, and not at the risk of the Council of the University of Southern Queensland, its Faculty of Health, Engineering & Sciences or the staff of the University of Southern Queensland.

This dissertation reports an educational exercise and has no purpose or validity beyond this exercise. The sole purpose of the course pair entitled "Research Project" is to contribute to the overall education within the student's chosen degree program. This document, the associated hardware, software, drawings, and other material set out in the associated appendices should not be used for any other purpose: if they are so used, it is entirely at the risk of the user.

Certification of Dissertation

I certify that the ideas, designs and experimental work, results, analyses and conclusions set out in this dissertation are entirely my own effort, except where otherwise indicated and acknowledged.

I further certify that the work is original and has not been previously submitted for assessment in any other course or institution, except where specifically stated.

Paul B Hohenhaus

08529465

_____

Signature

_____

Date

Acknowledgements

The author would like to acknowledge the assistance and support received throughout the course of the project. Sincere thanks are offered to the following people:

Dr Leslie Bowtell (USQ)

For his assistance and guidance throughout the project; the knowledge and real world experiences proving to be invaluable; the flexibility in organising meetings on an already busy schedule; and his enthusiasm around an industry base topic.

Mr Robert Coggan (Ergon Energy Corporation)

For conceiving the project topic; providing the resources; and his passion and knowledge of the topic; and most of all for his continual support, guidance and belief throughout the project.

Mr Scott Marsh (Ergon Energy Corporation)

For his continual friendship support and guidance throughout the project and helping to maintain the balance.

Mr Russell Wilson (Ergon Energy Corporation)

For his continual support and help during the length of the project

My family

For their patience, belief and the unconditional love throughout the project. My love and extreme gratitude go to my wife, Simone and my two most proud achievements, Blake and Lucas.

Table of Contents

List of Tables

List of Figures

Glossary

ACR	Automatic Circuit Recloser
A/D	Analogue to Digital
AS	Australian Standards
CAPEX	Capital Expenditure
DNSP	Distribution Network Service Provider
DR	Draft
PC	Personal Computer
PDS	Protection Database System
PSR	Protection Setting Request
IDMT	Inverse Definite Minimum Time
IED	Intelligent Electronic Device
I/O	Inputs / Outputs
LAB	Laboratory
LBS	Load Break Switch
LOI	Loss Of Current
LOV	Loss Of Voltage
MC	Maintenance Corrective
MF	Maintenance Forced
NER	National Electricity Rules
NERC	North American Electricity Reliability Corporation
OPEX	Operational Expenditure
OT	Over Time
PSR	Protection Setting Request
SCADA	Supervisory Control and Data Acquisition
SPE	Senior Protection Officer

SQL	Structured Query Language
SWP	Standard Work Practice
TC	Test and Commission

Chapter 1

Introduction

1.1. Chapter Overview

Provides the necessary background information relating to remote configuration of protection IEDs installed on the distribution network; justifying the need to progress the project, stating the project objectives and summarising the structure of the dissertation.

1.2. Project Overview

In the power industry, protection schemes that are installed to protect electrical plant and the public from power system events can be described as safety systems. These schemes historically consisted of electromechanical and solid state relays that were discreet devices used to detect power system faults and by design need ancillary equipment to provide additional control functionality. In the early 1980s digital/numerical protection relays where introduced as the next generation in relaying technology.

Today numerical devices are referred to as intelligent electronic devices (IEDs) and are software dependant which require single or multiple configuration files to apply predetermined thresholds and scheme logic to detect and operate for power system events. In a similar evolution to that of Programme Control Logics (PLC's) the addition of functional logic has presented new opportunities to manage more parts of traditional hardwired protection and control systems within software generated IED configuration files.

Power utilities have embraced IED technology by taking advantage of their integrated functionality. However, there has been concern within the industry of the use of remote management processes to provide alternate verification techniques of device protection functions (CIGRE Working Group B5-09 2006). More than ever network service providers are under increasing pressure to provide a higher quality of supply with lower operational (OPEX) and capital (CAPEX) expenditure. Ergon Energy uses IED technology in their safety related systems to further improve data capture and remote monitoring of their distribution networks; with the use of remote management techniques has been restricted to system event recording and control functionality.

Implementation of a more comprehensive remote management process introduces new challenges to ensure the safety system is commissioned, maintain and operated in a manner which complies with best practice and social expectations. To expand the use of remote management IED technologies power utilities will need an understanding of the processes required to maintain quality management of these safety systems.

1.3. Project Aim

The aim of this project is to assess the systems, processes and design criteria that will facilitate remote management of protection, monitoring and control infrastructure used on typical distribution network; and through assessment determine whether a configuration management process can be developed to reduce on-site commissioning and operational works on the existing population of Protection IEDs installed on the Ergon Energy network.

1.4. Project Background

Power utilities are under increasing pressure to provide a reliable and safe operation of their power network whilst delivering reduced operational and capital expenditures. To accommodate these expectations efficiencies in existing infrastructure and operating techniques warrant continual examination. One area that has potential for increased efficiencies for Ergon Energy is the remote management of Intelligent Electronic Devices (IEDs) used to monitor and protect its distribution network. Communication infrastructure already exists to provide connectivity to protection IEDs located in

substations and on pole mounted installations facilitating SCADA and remote engineering access.

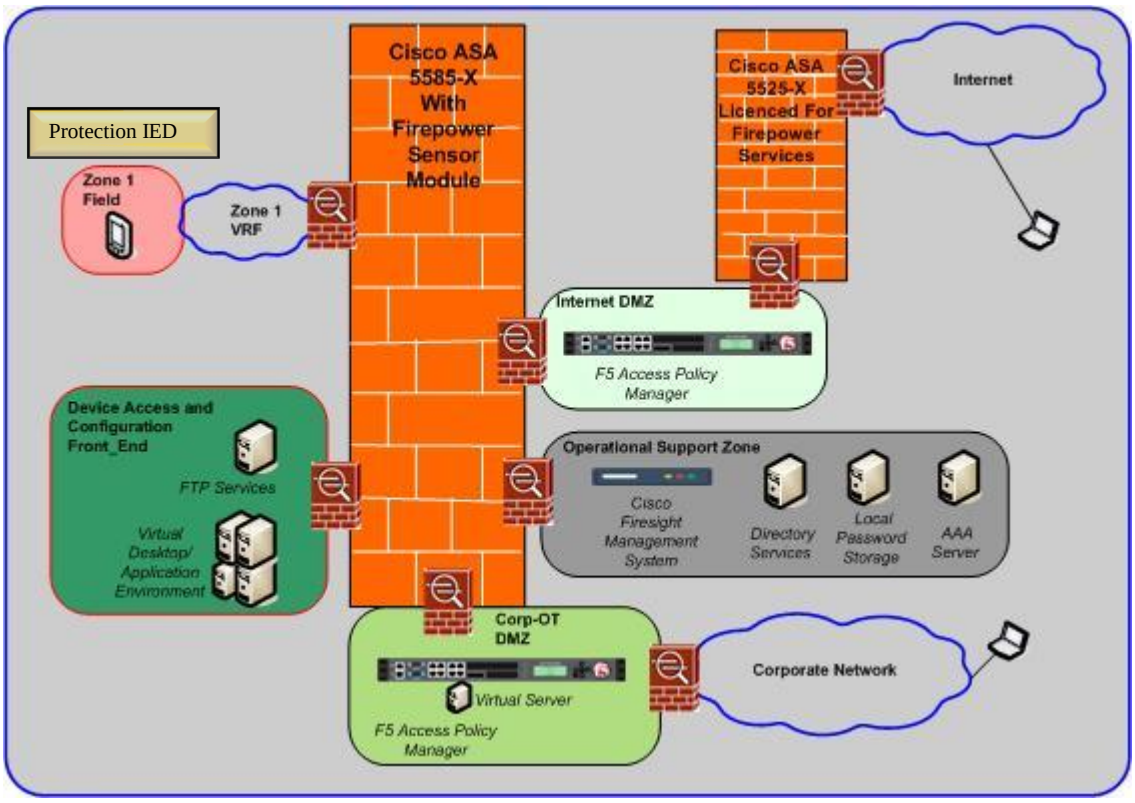


Figure 1: Existing connectivity infrastructure on the distribution network

SCADA connectivity provides control and monitoring of installed protection IEDs by publishing alarms, power system measurements, and associated plant status to a centralised operational control centre. Remote engineering connectivity provides protection engineers' access to Protection IEDs as if the protection engineer was standing in front of the device. This in theory allows the engineer to read and write a configuration file to the Protection IED, extract event and disturbance recordings, and perform control and monitoring operations similar to that of the SCADA connectivity. However existing Ergon Energy's remote management processes restrict the interaction to the Protection IED to on-line monitoring and retrieval of power system disturbance and event records.

1.5. The Need for the Project

Ergon Energy currently has towards approximately 4,600 Protection IEDs connected to a communication infrastructure. For the purpose of this project these devices have been categorised into three different types in terms of their application and functionality;

- **Basic** IEDs – Devices with fixed functionality with configuration parameters typically limited to the ranges and resolutions required to define a protection trip characteristic. Examples of these devices are ACRs and sectionalisers.

- **Intermediate** IEDs – Devices that typically have similar configurable ranges and resolutions as the Basic IED with the addition of configurable functionality such as programmable logic and I/O (Inputs/Outputs). Examples of these devices are distribution feeder management protection relays used within a Substation environment.

- **Integrated** IEDs - Fully integrated IEDs with similar capabilities of that of the Intermediate IEDs which are communicating peer to peer with other protection device. Examples of these devices are line differential relays which require communication connectivity between two substations or IEC61850 devices employing GOOSE.

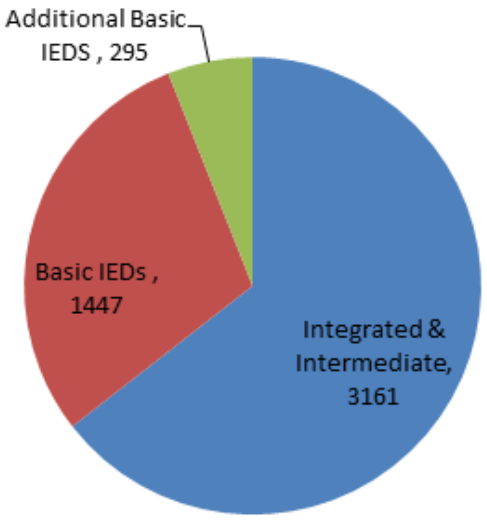


Figure 2: Quantities of Protection IED types on the Ergon Energy network

A population of 1447 ACRs (Basic IED) installed throughout Ergon Energy's distribution network and a further 295 expected to be installed by the end of 2015 highlights the reason to examine alternative configurable management processes. Using existing communication infrastructure to reduce operational delays, costs and travel for staff operating under the current IED configuration processes is expected to allow better management of the geographically diverse population of ACRs.

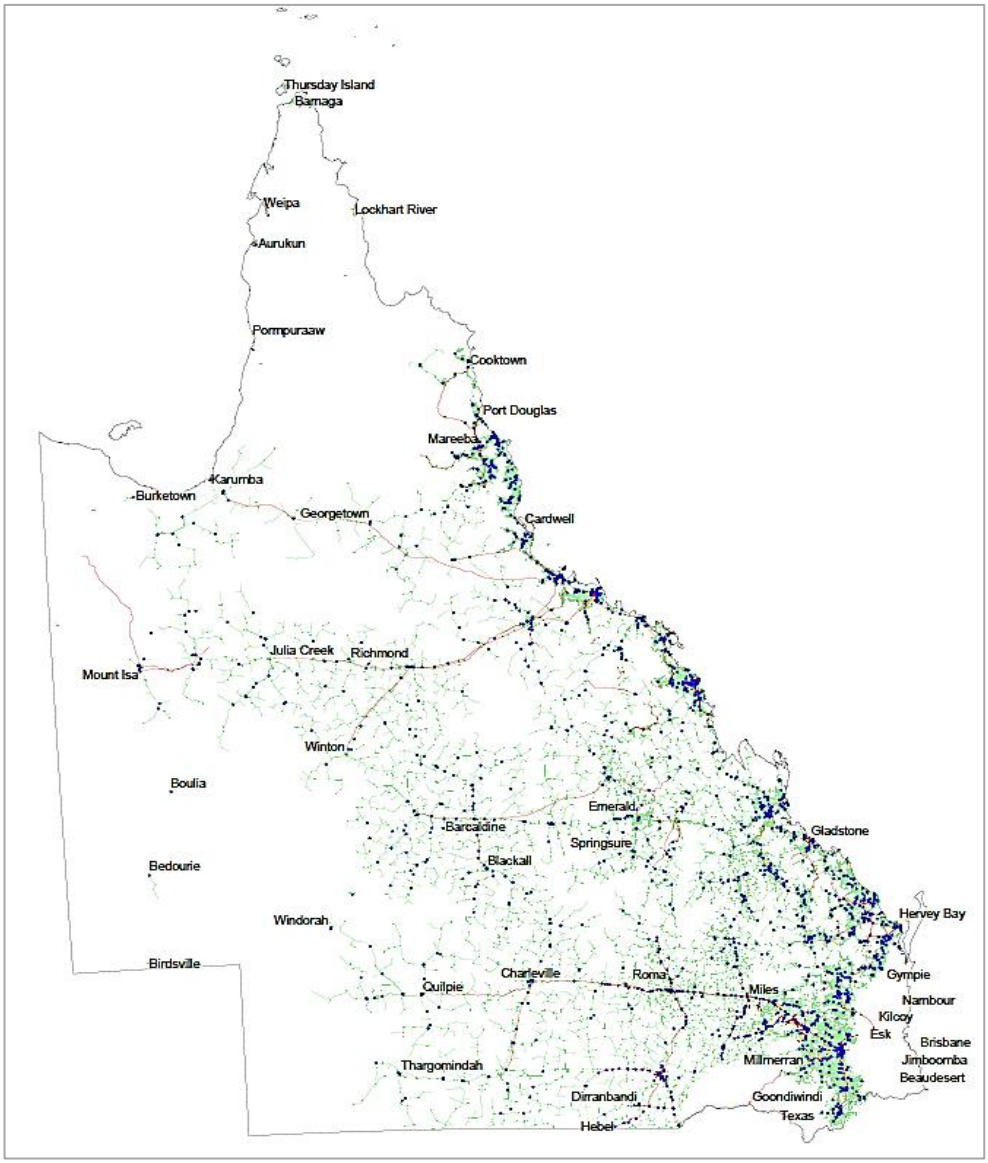


Figure 3: Location of Basic IEDs installed across the Ergon Energy network

The blue dots in Figure 3 identify the location of the 1447 ACRs (Basic IEDs) across Ergon Energy's distribution network. Test staff employed to undertake reconfiguration of these pole mounted Protection IEDs are based in six central locations; Brisbane, Toowoomba, Maryborough, Rockhampton, Mackay, Townsville and Cairns; mobilising staff to rectify a protection setting introduces delays.

Owing to the geographical diversity of Ergon Energy's distribution network a request to initiate a remote change to an IED is inevitable, that is, can a protection setting be changed on-line? To better understand and acknowledge the risks associated with remote configuration management; and to be able to respond to these requests the project investigated three areas of the configuration management process with an aim of driving quality Protection IED configurations and where possible deliver these configuration files through the existing communication infrastructure.

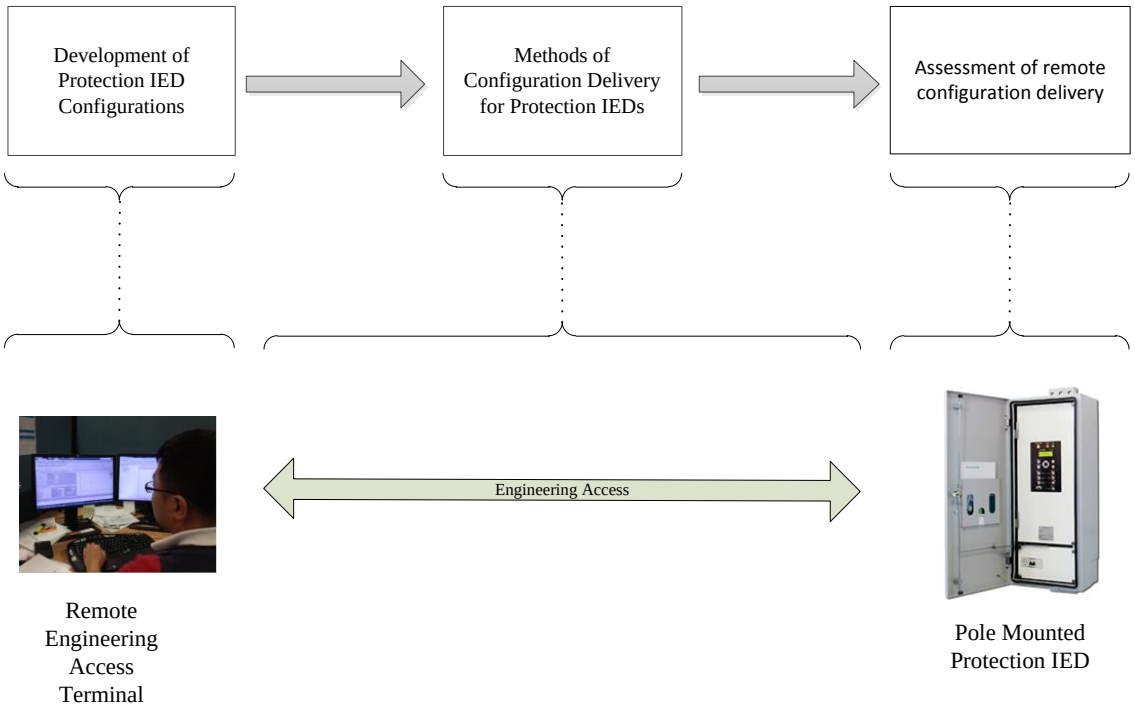


Figure 4: Development phases for remote configuration management

1.5.1. Development of Protection IED Configurations

Configuration quality at the IED level involves developing IED configurations that are of an inherent accuracy that would ensure:

- Post deployment testing of the configuration would not identify any issues that were within the control of the personnel responsible for the configuration development.
- The configuration is correct for the installation and the plant item being protected.

The work undertaken in this area involved reviewing and assessing existing configuration management processes used in Ergon Energy. With the outcome benchmark further improvements applied to the existing workflow addressing, but not limited to, the following key points;

- Ensures minimum Industry performance standards are met.
- Applies a quality management approach to the alternate configuration strategy.
- Identifying and managing the source of any errors

1.5.2. Methods of Configuration Delivery for Protection IED

The ability to ensure the configuration is able to be delivered consistently and confidently to the intended Protection IED is identified as the next step in remote configuration delivery. The work undertaken here centred on developing processes that clearly defines alternative verification methods that will support remote configuration delivery whilst complying with required regulatory, legislative and industry requirements.

1.5.3. Assessment of Remote Configuration delivery

For the purpose of this project Intelligent Electronic Devices (IEDs) will be considered to consist of two components, the first is the software and the second is hardware. Each is equally important to understand the effect of remote reconfiguration and the minimal requirements needed for operational remote changes to the protection IED. The firmware and software which are directly related to the protection IED configuration file are both addressed within the configuration delivery process. The hardware pertains to components that are critical for its operation and include but not limited;

- A/D converters used for power system measurements
- Power supply
- Functional inputs/outputs (I/O) that receive and send signals to ancillary control equipment to operate primary plant.

Methods to determine the Protection IED's health at the time of delivery and how it responds to a configuration request was also examined. This was considered owing to traditional practices incorporate health checks as part of their configuration delivery whilst the Protection IED is isolated from the network and field staff are on site. The project is investigating methods of delivery of the configuration file whilst the protection IED remains in service from a remote location. Understanding the impact of limiting this could have on its primary function of protecting the distribution network.

1.6. Project Objectives

The aim of the project is to identify and document a number of strategies and their limitations to enable effective and efficient remote management of protection IEDs currently used on the Ergon Energy network; with the objective to develop opportunities to reduce operational delays where reconfiguration is required for installed protection IEDs. Although Ergon Energy uses three types of protection IEDs as outlined in section 1.5 the objectives of the project will initially explore the requirements needed to develop a configuration management process for the Basic IED type owing to the following;

- The characteristics of a Basic IED configuration forms the basis of all types of protection IEDs used on the Ergon Energy network.
- The increase in ACR numbers dispersed across a large geographical area.

The following objectives were identified to deliver a successful project (the objectives are also described in the *Project Specification* in Appendix A.

1) Identify existing work flows of Ergon Energy's current configuration development and research the effectiveness of current management strategies through analysis of survey and internal non-conformance logs

2) Investigate methods for setting verification

3) Design a new IED configuration delivery process and analyse its efficiency and effectiveness against existing processes established in (1).

4) Research and evaluate an alternate method to support remote configuration verification of selected protection IEDs used on the Ergon Energy network.

5) Research and test how selected IEDs respond to configuration delivery whilst remaining in service.

6) Development of risk matrix to be used for remote configuration delivery

Objectives 1, 2 and 3 involved the development of a configuration management process to ensure configuration files can be delivered for each Protection IED type consistently and free of error. This establishes the first step in developing confidence in delivering configuration files that are fit for purpose and will operate as intended. Items included in this work, but not limited to, were;

- Establish methods to track the quality of IED configurations
- Analysis and improvement of existing workflows

Objective 4 involved development of an alternate method that can be used to successfully deliver a configuration file through a remote management process. Items included in this work, but not limited to, were;

- Establish the requirements needed for operational changes for the Basic IED type
- Ensuring compliance with existing legislative requirements and relevant Industry Standards maintaining best practices.
- Evaluate available methods of the verification of installed configuration files.

Objectives 5 and 6 involved the development of risk assessment matrix to evaluate the use of the remote management process for reconfiguration of the Basic protection IED for day to day operations. Items included in this work, but not limited to, were;

- Understanding and evaluating how a selected manufacturer's IEDs responds to a configuration change during remote delivery with the aim to identify the requirement to apply similar criteria on other protection IEDs exposed to the same process.
- Risk assessment matrix that bounds and evaluates the remote management process for reconfiguration operations.

1.7. Overview of Dissertation

Chapter 2 – Literature Review: Presentation of all relevant literature for the purpose of developing processes and methods to establish a remote configuration management processes for selected protection IED applications.

Chapter 3 – Methodology: A statement of the planed approach to successfully fulfil the objectives described; from improving configuration accuracy to identifying the challenges associated with remote delivery to selected protection IEDs.

Chapter 4 – Configuration Management: Identifies and assess existing configuration management processes identifying root causes of configuration error and how these may be managed by the design of improved setting delivery process.

Chapter 5 – Remote Delivery of IED Configurations: A review of the Queensland regulatory and legislative requirements for Protection IED testing for Distribution Network Service Providers (DNSPs); combined with the examination and assessment of the comparison between the traditional and the alternate delivery process.

Chapter 6 – Response to Setting Changes: Details the laboratory testing of a selected protection IED to assess how the device responded to external influences that may occur during a remote configuration delivery, including how reconfiguration differs whilst the protection IED remains in service.

Chapter 7 – Operational Risks: Detailed discussion on the operational risks associated with remote configuration and the recommended actions that should be undertaken to confidently remotely deliver a configuration to a selected Protection IED.

Chapter 8 – Feasibility of Remote Configuration: A comparison of costs associated between the traditional and remote delivery processes to apply configuration files into installed Basic IEDs.

Chapter 9 – Conclusions & Recommendations: An assessment of the degree of success in delivering the described objectives including future works.

1.8. Limitations & Restrictions

The following limitations and restrictions will apply to the project and dissertation.

- To comply with confidentiality and security restrictions detailed information involving Ergon Energy's communication infrastructure will not be disclosed within this dissertation.

1.9. Chapter Summary

The chapter has provided an introduction and background into this dissertation introducing the Protection IED's use and importance within the industry. Continual focus on distribution network service providers' operational and capital expenditure highlights that an effective remote management strategy has the potential for Ergon Energy to maintain existing maintenance schedules at reduced costs and improve operational flexibility.

The increasing numbers of protection IEDs being installed onto Ergon Energy's network advocates assessment and where possible improve current processes to enable effective and efficient remote management; and where appropriate reduce operational delays. The chapter outlines the objectives of the project and concludes with describing three key areas that were considered essential to assess the opportunity to deliver a remote configuration management process.

Chapter 2

Literature Review

2.1. Chapter Overview

To obtain an understanding of the current practices and the requirements needed to implement a remote engineering and configuration management process a literature review was undertaken in the following areas;

- Relevant Standards
- Legislation requirements of safety related systems
- Configuration Management Strategies
- Protection IED Configuration Management
- Methods for assessing risk for process systems
- Setting errors in safety related systems

2.2. Relevant Standards

To further examine whether a remote management strategy can include online configuration legislation compliance is essential (Electricity Act, 1994) ensuring any proposed strategy is benchmarked against relevant Australian Standards.

2.2.1. AS 61508.1

Australian Standards AS61508.1 details the functional safety of programmable electronic safety-related systems. The standard prescribes the management of functional

safety, safety lifecycle requirements and methods of developing validation processes for safety related systems.

One section of particular interest for the progression of the project is section 6 which discusses the management of functional safety. The standard discusses procedures that shall be employed for effective functional safety which include;

- hazard and risk analysis
- functional safety assessment
- verification activities
- validation activities
- configuration management
- incident reporting and analysis

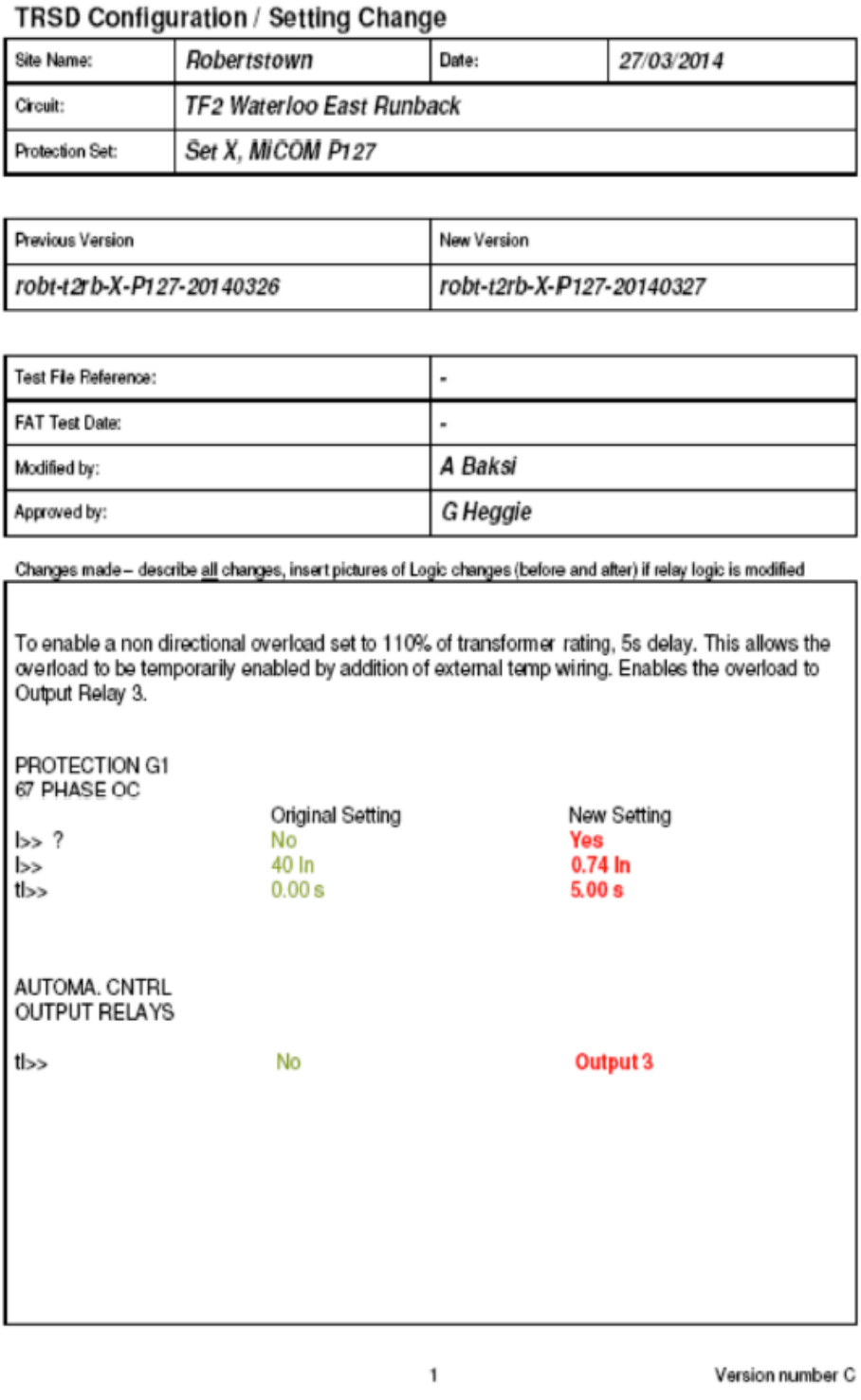
Clause 6.2.10 relates to configuration management discussing the procedures that are to be addressed with regard the safety related system. This clause was relevant to the project and provided guidance in developing mechanisms for software verification and management.

Clause 6.2.8 discusses procedures that should be developed for the modification of a safety related system and ensuring the appropriate approval and authority has been obtained. This consideration has relevance to the project with respect to identifying the necessity for change. Though a remote configuration management process may provide the mechanism to allow a change to a Protection IED there also needs to be a critical assessment for the need to change. If deemed appropriate documentation should be developed to capture the how, what, who, when and why of the remote reconfiguration.

At the 2015 SEAPAC conference a paper was (Heggie, 2015) delivered discussing methods undertaken by ElectraNet to modify limited functions of a protection IED from a remote location. The paper also provided what would be considered as a working example of the required documentation needed to record the process of the modification of a Protection IED as shown in Figure 5.

This example clearly captures the how, what, who, when and why for the protection IED under modification. The paper further discusses ElectraNet's process of verification and validation methods used during remote modification of Protection IEDs

providing additional opportunity to bench mark the project's proposed configuration management process against other Australian utilities.



TRSD Configuration / Setting Change

Site Name:	*Robertstown*	Date:	*27/03/2014*
Circuit:	*TF2 Waterloo East Runback*		
Protection Set:	*Set X, MiCOM P127*		

Previous Version	New Version
robt-t2rb-X-P127-20140326	*robt-t2rb-X-P127-20140327*

Test File Reference:	-
FAT Test Date:	-
Modified by:	*A Baksi*
Approved by:	*G Heggie*

Changes made – describe all changes, insert pictures of Logic changes (before and after) if relay logic is modified

To enable a non directional overload set to 110% of transformer rating, 5s delay. This allows the overload to be temporarily enabled by addition of external temp wiring. Enables the overload to Output Relay 3.

PROTECTION G1
67 PHASE OC

	Original Setting	New Setting
I>> ?	No	Yes
I>>	40 In	0.74 In
tI>>	0.00 s	5.00 s

AUTOMA. CNTRL
OUTPUT RELAYS

tI>>	No	Output 3

1 Version number C

Figure 5: ElectraNet IED modification document example (Heggie, 2015)

2.2.2. AS 61508.3

Australian Standard AS 61508.3 prescribes software requirements for functional safety of programmable electronic safety-related systems. In particular the standard describes tasks that should be considered for developing validation plans for software used for safety related systems. A detailed review of this standard will be undertaken to help develop verification methods of the software used within the remote management strategy.

2.2.3. AS 2067

The published Australian Standard AS2067-2008 "Substations and high voltage installations exceeding 1kV a.c." currently provides little guidance around protection systems installed within a substation environment. However the standard is currently under review and the first draft DRAS2067:2014 was issued to the industry in January, 2015 for comment; with new clauses and sections added and in particular Appendix F which discusses the requirements and considerations for power system protection. The parts of particular interest for this project are;

- F6.12 Protection relays and systems
- F6.13 Verification of relay settings

Ergon Energy was given the opportunity to formally respond to the draft in whole which was excepted and comments were provide in parts where improvements could be made to align with current and future industry practices which included the aforementioned parts of Appendix F .

2.2.3.1. F6.12 Protection relays and systems

The proposed Appendix F discusses the need for regular intervals of functional testing of protection relays to ensure a high degree of dependability. The suggested method to totally prove the protection relay's functionality should involve the injection and measurement of the configured operating quantities (DRAS2067:2014).

Schweitzer Engineering Laboratories suggests regular intervals of simulated injection to verify protection IED functionality is not required if the protection IED is

comprehensively tested and commissioned at the time of installation; and a management program is employed to monitor the following (Zimmerman, 2014);

- Relay self-test alarm contact in real time via supervisory control and data acquisition (SCADA) or other monitoring system
- Potential relay failures not detected by self-tests
- Analyse event reports to root cause, and verify logic inputs and output contact operation.
- Observe and act on all product service bulletins.

From this it is evident that manufactures are confident that products will operate effectively and confirmation of protection IED functionality without the need to provide external simulation is possible.

Ergon Energy currently follows similar methods outlined in the draft clause F6.12, that is, commissioning Protection IEDs prior to placing them into service; and maintains a regular maintenance program on Protection IEDs located in substations. Pole mounted Protection IEDs are also fully commissioned at the time of installation.

Ergon Energy representatives were asked to respond to the draft standard DRAS2067:2014 with a considered response that aligned with the those outlined in the Schweitzer Engineering Laboratories White paper (Zimmerman 2014). However caution is needed when applying these methods as each manufacturer's self-monitoring abilities will vary. Assessment of manufacturer's recommendations will be important in future product selection.

How this clause progresses through to its final publication of AS2067 could eventually influence the outcome of the projects' objectives two and three outlined in section 1.6. It is envisaged that the final standard of AS2067 will not be published prior to the completion of the project; therefore it would be recommended that review of the strategy should be undertaken on the final publication of AS2067 ensuring the strategy remains complaint with respect to those areas aligned to the new standard.

2.2.3.2. F6.13 Verification of relay settings

Clause F6.13 states reliance for correct operation should not depend on settings established solely by downloading settings or by positioning dials and plugs (DRAS2067:2014). In addition the verification of a setting should be tested and confirmed by secondary injection.

This clause does pose some challenges with regard to remote setting changes owing to the suggestion protection related functions should be tested by methods involving a physical presence with the device. Development of an alternate verification process will need to encompass the means to test the applied settings to ensure they are operational and fit for purpose in preparation of this clause being published without change in the final print of AS2067.

Ergon Energy also responded to the draft standard with suggested changes to the proposed wording in section F6.12 to recognise that today's protection relays are not based on traditional voltage and current measurements i.e. numerical devices that use A/D converters to measure the applied current and voltages aligning with current technologies.

2.3. Legislative/Regulatory Requirements

A review of legislative requirements in Queensland for testing of safety systems was undertaken to determine the limitations, if any, when incorporating commissioning and operational works within the remote management strategy. A review was undertaken on the following Legislation;

- Work Health and Safety Act 2011 of Queensland
- Electricity Act 1994
- Electricity Regulation 2006
- Electrical safety code of practice 2013
- National Electricity Rules (NER)
- Electrical Safety Regulation 2013
- Nation Electricity (Queensland) Law: Current 19 19/12/2013

2.3.1. Legislation requirements for testing of safety related systems

A Distribution Network Service Provider (DNSP) must protect its supply network to ensure a safe connection and supply to its customers and also comply with any directives outlined in the National Electricity Rules (Electricity Act, 1994). Distribution Network Service Providers must also maintain a compliance program to ensure that its protection systems operate reliably (National Electricity Rule, V65). These mentioned legislative compliances do not instruct utilities on the method or frequency of testing of installed protection schemes. To compensate utilities have traditionally used years of design and operational experience to understand the failings of applied protection scheme to collate and construct maintenance programs deemed to meet with the required legislation.

Review of the Electrical Safety Regulation 2013 identified in Part 11- Safety management systems Section s234, part 3(b) which states;

(3) *When a prescribed electricity entity's safety management system is first put into effect or is modified, the entity must give the regulator—*

(b) *a certificate in the approved form from an accredited Auditor that verifies the safety management system has been assessed and validated to ensure the system comprehensively identifies and addresses the hazards and risks associated with the design, construction, and the operation and maintenance of the entity's works.*

Section s234 highlights the need to obtain and review Ergon Energy's safety management system to assess the hazards and risks that are documented especially around design, operational and maintenance of the entity's works to ensure the project objectives are compliant with what is currently lodged with the regulator. Where the Project's objectives are found to impact Ergon Energy's safety management system full disclosure of the non-compliance shall be documented.

Further review found in Division 2 – Earthing and Protection, Section s198 – Performance and other requirements for works, part (h) which states;

The following requirements apply for the works of an electricity entity—

(h) electrical equipment intended to form part of the works of an electricity entity must undergo commissioning tests and inspection to verify that the electrical equipment is suitable for service and can be operated safely when initially installed or altered.

The process of configuring a protection IED remotely will need to clearly identify the mechanisms to verify and confirm the configuration delivery in a manner which is consistent with existing industry practices and also complies with section s198 of the Electrical Safety Regulation 2013.

2.4. Development of Configuration management strategies

A detailed examination of the lifecycle of configuration files will help develop and understand the complete workflow needed to produce and maintain these files. During the life time of the protection IED power utilities need to consider development of quality assurance processes which simplifies the setting management process, minimises the possibility of human error and provides an auditable record of any changes implemented (CIGRE WG B5.31, 2013). Figure 6 displays an example of a generic process for managing lifetime settings (CIGRE WG B5.31, 2013).

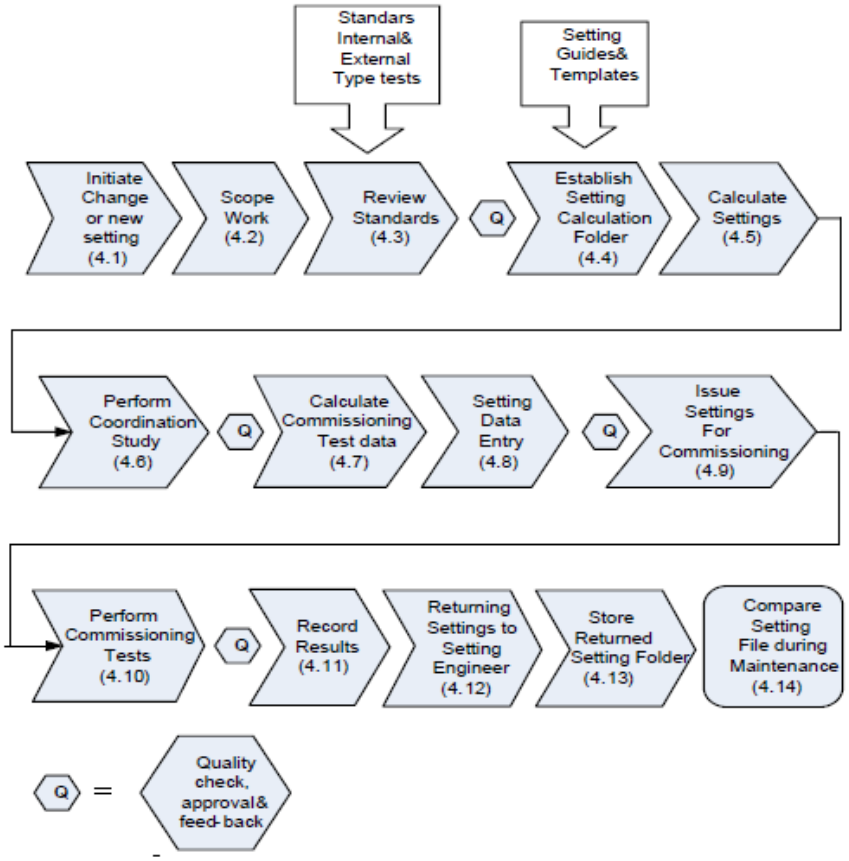


Figure 6: Generic process for managing lifetime of settings (CIGRE Working Group B5.31 2013)

Strategies to provide remote management of safety systems will need to incorporate processes to support (CIGRE, B5.205, 2008);

1) Change Management – Processes to ensure protection IED identification is maintained and verified during failed in-service or upgrade conditions.
2) Risk Reduction – to reduce risks caused by changes may be reduce by the combination of appropriate requirements for software protection, software examination and software conformity.
3) Data Handling – encompass the areas of long term data storage and remote download of software and/or firmware.
4) Version Control – is essential to provide reliable operations of the safety systems during commissioning, maintenance and operation. Due to the complexity of interrelated processes involving field maintenance and commissioning of these systems, it will be essential to have the ability to track changes implemented, where it was implemented and by whom (CIGRE , WG B5.09, 2006).

A recurring theme of on-line/remote management techniques, whether it is around remote testing or data retrieval, is the need for standardisation. Standardising configurations of protection relays minimises design mistakes and human errors and will deliver similar behaviour from similar types of IEDs (B5.227, CIGRE 2014). Standardisation also needs to extend to the delivery of the configuration files and the verification tests required for each style of IED installed. (Kezunovic, M. 2002). Ergon Energy has embraced similar philosophy and has implemented standard applications for all protection IEDs purchased on recent period contracts.

However where the intermediate and integrated type IEDs are installed into brown field sites (Non-standard applications) there is not the same rigour around documenting configurations expected for these applications. For these applications the protection setter is required to deviate from the prescribed standard imposing additional functions and features to the protection IEDs configuration. Therefore it is essential to consider techniques for both standard and non-standard applications in developing the methods to provide a universal configuration management process.

To progress the opportunity of performing on-line reconfiguration of selected protection IEDs, surveys of field staff were undertaken, focusing on configuration file delivery as

well as areas of human error that may exist within the existing configuration file workflow. These errors can then be aligned with tasks within the workflow and their risk ranked with respect to the impact of the functionality under change (Liang, Lin, Hwang, Wang, Patterson, 2010). Success of on-line reconfiguration depends on how the remote management process can mitigate the risks identified and the rigour around its auditability (Heggie 2015).

2.5. The Importance of Settings in Safety Related Systems

2.5.1. What's in a setting?

The importance of bounding and understanding a setting within a safety system is demonstrated in findings delivered from the enquiry into the 1998 Esso gas plant at Longford in Victoria. The enquiry found procedural, maintenance, auditing and management deficiencies all contributed to a fractured gas vessel causing an explosion killing two men, injuring 8 others and cutting Melbourne's gas supply for two weeks. The accident sequence started owing to a frequently ignored alarm which allowed plant processes to operate outside required parameters. This was identified as common practice owing to the sheer volume of frequent alarms and operators came accustomed to the plant operating in constant alarm mode for long periods although some alarms may have been tolerable operators had no way of distinguishing between critical and non-critical alarms.

"*One alarm in particular was frequently ignored. It concerned the level of condensate liquid in a certain vessel. This could be measured up to so-called 100per cent level. Higher levels were physically possible but were not measureable. The alarm was set at the 85 per cent level"* (Andrew Hopkins, 2000, p.41)

The Esso incident involving safety systems highlights the need to have some measure of validity of the thresholds configured within protection IEDs installed on Ergon Energy's distribution network. One method is to determine a process to benchmark those settings that are deemed appropriate for each application before they are applied to the network.

"*It is clear that, had engineering staff been working with operators on a daily basis, the practice of operating the plant in alarm mode for long periods could not have developed in the way it did."* (Andrew Hopkins, 2000, p.49).

Historically determining whether a protection setting was deemed appropriate for its application has relied on the experience and the knowledge of Ergon Energy's protection engineers. Where this experience is not accessible or where external companies are engaged to perform similar work the depth of knowledge and experience of the protection engineer is unknown. In these cases a reliable verification method is needed further supporting the need to have some mechanism for validation.

Another example is the 1965 black out in the Northwest of the United State which left over 30 million people and 270,000 square kilometres without electricity for 13 hours was due to a setting that was established 7 years prior and was never checked to be correct before the system loading condition which contributed to the event (CIGRE Working Group B5-09 2006).

2.5.2. Misoperations of Protection IEDs

The paper "Protection System Mis-operation Analysis" describes the leading causes of 2,200 protection mis-operations across the North American continent since 2011 collated by transmission, generation and distribution providers and their finding reported to the North American Electricity Reliability Corporation (NERC). "Approximately 65% of the misoperations occurred due to three leading causes which are incorrect settings/logic/design errors, relay failures/malfunctions, and communication failures" (Bian, Slone & Tatro 2014)

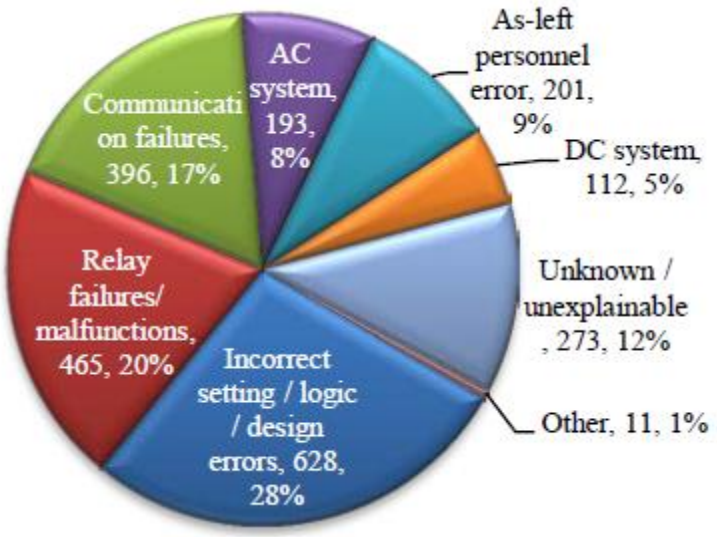


Figure 7: NERC – Misoperations by cause (Bian, Slone & Tatro 2014)

"*Microprocessor relays have a higher number of misoperations attributed to settings/logic/design errors compared to the other technologies"* (Bian, Slone & Tatro 2014).

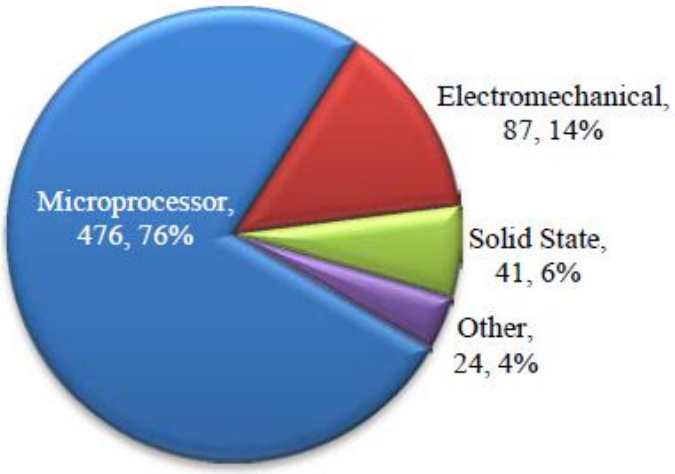


Figure 8: NERC – Misoperations by technology type (Bian, Slone & Tatro 2014)

Sections 2.5.1 and 2.5.2 highlight the importance of delivering a configuration file containing as little error as possible. The data presented in Figure 7 further reinforces the need to examine the quality of configuration development in determining appropriate methods to reduce the frequency of error and increase confidence in the configuration delivery. From Figure 8 it is obvious the microprocessor relays (IEDs) introduce additional complexity and setting challenges increasing the possibility of errors compared to other technology types.

Protection System Mis-operation Analysis (Bian, Slone & Tatro 2014) findings were used in developing a perception survey that was distributed to Ergon Energy's field test staff to assess the effectiveness of the existing configuration delivery process.

Though the perception survey differs from the NERC paper (Bian, Slone & Tatro 2014), as it is designed to report on errors found during functional testing, it is considered it has identify those errors that if left unchecked would inevitably lead to mis-operations. This paper provides an opportunity to provide a comparison of the data obtained from the Ergon Energy survey and may provide a method of benchmarking of settings/logic/design errors against other power utilities.

2.6. Remote Configuration of Protection IEDs

The development of a remote management process provides the opportunities to reduce on site commissioning and/or operational visits. Expanding a remote configuration management process that facilitates changing settings on-line requires understanding of the Protection IEDs structure. Figure 9 is a typical layout of a digital protection IED which demonstrates it is convenient to consider these types of devices in three sections (CIGRE Working Group 34.10 2000):

1) Analogue Input section
2) Contact Input/Output circuitry
3) Processing data

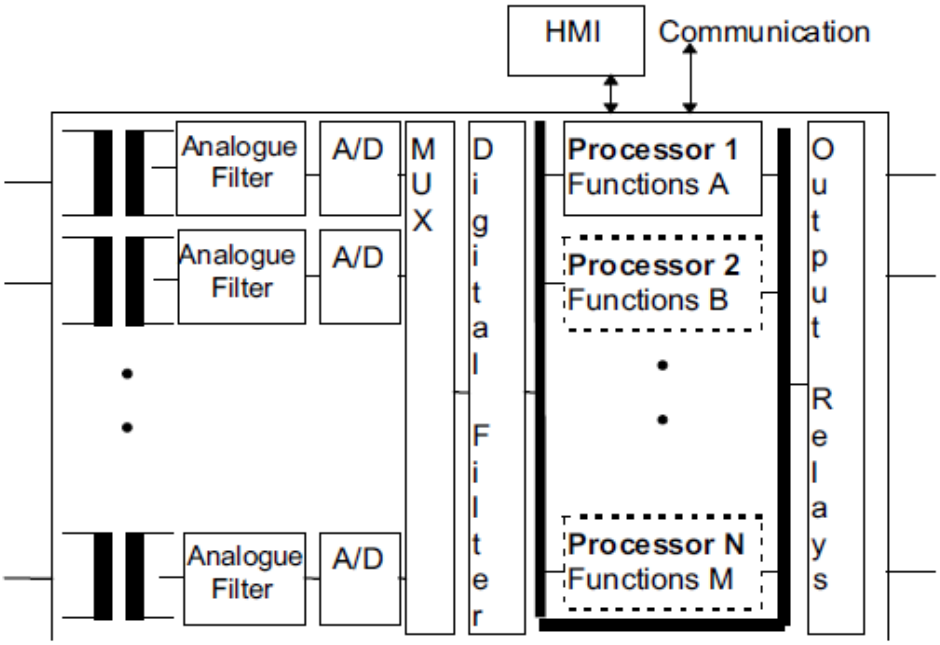


Figure 9: Typical layout of a digital protection system

These three sections can be reduced to consist of two components, the first is the software and the second the hardware. Each is equally important to understand the effect of remote reconfiguration and the minimal requirements needed for onsite commissioning or operational changes to the protection IED.

Configuration changes occur in vendor software creating a configuration file that is directly related to item 3) of the protection IED. To implement the required threshold and/or functionality the configuration file is created and written to the protection IED's processor. The hardware pertains to items 1) and 2); the functional inputs and outputs (I/O) that receive and send signals to ancillary equipment to operate primary plant; as well as the A/D converters and filters used for the analogue measurements.

This structure highlights how remote configuration may not just be a single process to ensure the protection IED is operational. A concert of processes may be required prior, during or after the configuration file has been delivered to ensure confidence in correct operation of protection IED.

2.6.1. Verification for Protection IED Operation

An Ergon Energy standard STNW1156[1] prescribes a maintenance acceptance criterion which includes setting checks and functional testing of protection relays. The described testing requirements supports the need for a form of function tests to be performed ensuring hardware of the protection device is operating as designed. This prompted further research to identify other methods and/or practices that are being used to perform remote relay testing of protection IEDs within similar industries; or whether verification of these functions may be possible by other methods such as online inspection of the protection IED's response to measured power system faults, event recording and hardware alarm contacts.

2.6.1.1. Remote Testing

One method of remote testing reviewed (Musaruddin, Zaporoshenko, Zivanovic, 2008), prescribes installing and using proprietary equipment or simulators installed at the same location of the device in order to provide low level or what is commonly referred to as system testing to provide protection engineers an alternative to on-site protection IED troubleshooting. Implementing such methods to facilitate functional testing would impose significant expense considering the different makes of IED implemented across Ergon Energy's distribution network. In addition this method only supports those

[1] STNW1156 is an Ergon Energy Standard document deemed to be essential in addressing key goals for online IED configuration listed in the project objectives. This document is only available internally to Ergon Energy.

protection IEDs located in substation installations and would not be suitable or feasible for ACR Basic IEDs. This technique does not comprehensively test the scheme as it cannot isolate and operate outputs without additional hardware that will effectively reduce the inherent reliability of the system

2.6.1.2. Alternate Methods

The health of a protection IED refers to its ability to operate as designed. Historically routine testing of protection IEDs have been used to examine the health and operations by detecting protective relay failures of those three sections shown in Figure 9. The only other option provided to the user is to observe mis-operations during power system faults by the use of events captured by the protection IED (Kumm, Schweitzer & Hou 1995). The amount of testing and the frequency of testing to detect these failures have historically been left to the DNSP to decide in consideration of legislative and regulatory requirements; and manufacturer's recommendations. Routine testing, though by design is quite thorough, but if not balanced it is time consuming and costly on an increasing population of Protection IEDs.

A recent SEL white paper discussing the recommendations for maintenance testing (Zimmerman 2014) describes a number of mechanisms that can be used to establish the Protection IEDs ability to operate for power system faults. The paper describes where the Protection IED has been comprehensively commissioned for its application at the time of installation the use of self-monitoring and alarms to detect relay failure may be used to reduce the frequency of maintenance. The paper also discusses the importance to have additional mechanisms to verify those functions that cannot be fully verified by self-monitoring.

The following is a suggested regime of tests that can be used to detect all relay failures in a typical protection IED (Kumm, Schweitzer & Hou 1995);

- Self-test alarm monitoring
- Loss of signal (LOV, LOI) monitoring
- Review of relay event reports

- Periodic checks of relay inputs and outputs[2]
- Periodic calibration check by comparison

The comparison between the digital relay self-testing and monitoring functions and traditional relay testing are shown in Figure 10 (Kumm, Schweitzer & Hou 1995). Highlighting opportunities to reduce on-site testing and at the same time provide alternative mechanisms to verify the complete health of the protection IED including alternate methods of hardware verification as part of a remote management process.

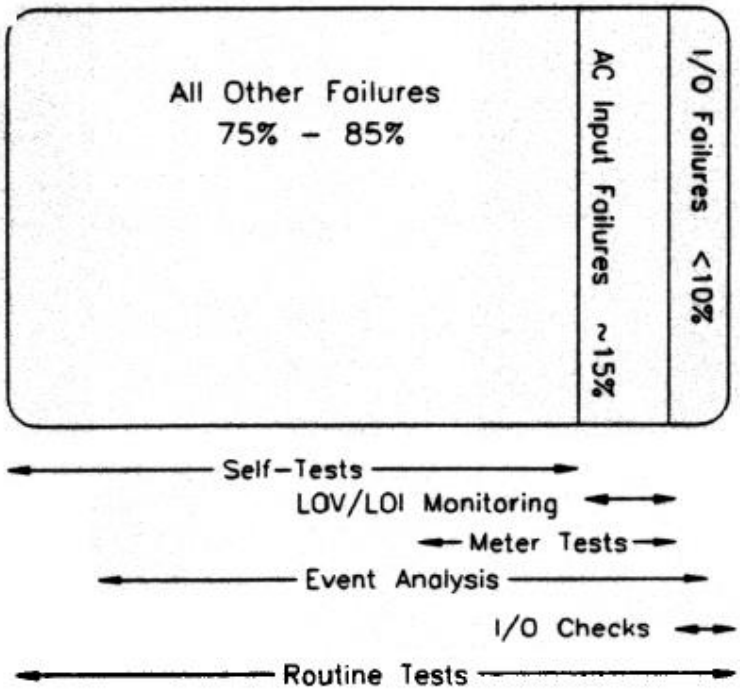


Figure 10: Digital relay self-testing and monitoring functions replace traditional routine tests

2.7. Protection IEDs Response to Setting Changes

Existing verification practices are performed on-site and always with the protection IED out of service or isolated so not to cause unwanted power supply interruptions. If the protection IED is taken out of service then the equipment or network it has been

[2] Where a protection IED is exposed to infrequent operation e.g. bus or transformer protection then other methods to verify the relay inputs and outputs would be required.

installed to protect may also be removed from service depending on availability of redundant protection schemes. A remote setting change may require similar redundancies as the setting change and verification process would need to occur whilst the Protection IED remains in service. Highlighting the importance to understand what affect this may have on the Protection IED and the equipment or network it is protecting during the remote configuration delivery.

The remote management of protection relays and discusses the risk of mal-operations by a microprocessor type protecting device during configuration file delivery is extremely low (Pingping & Guo 2014). The precursor to this statement is that the configuration file is correct for the application.

The paper does acknowledge that a risk of mis-operation exists and could occur if there was a fault on the network whilst the configuration file is being uploaded. This is due to the time taken for the protection settings to solidify (take affect) within the Protection IED. How long this takes would vary from manufacturer to manufacturer and could range between milliseconds to two seconds (Pingping & Guo 2014). An example of this process is shown in Figure 11.

The times taken to solidify the protection change discussed in this paper are certainly values that would be of little concern for transmission networks within Australia owing to the mandatory protection scheme redundancy requirements (AEMC - Australian Energy Market Corporation 2014). For sub-transmission and distribution networks maximum times for Protection IEDs can depend on a number of conditions; some which include earth potential rises and plant and conductor damage and the same redundancy requirements are enforced. For devices that allow a setting change to be effected whilst a network fault exists, the effect on clearing time will need to be considered.

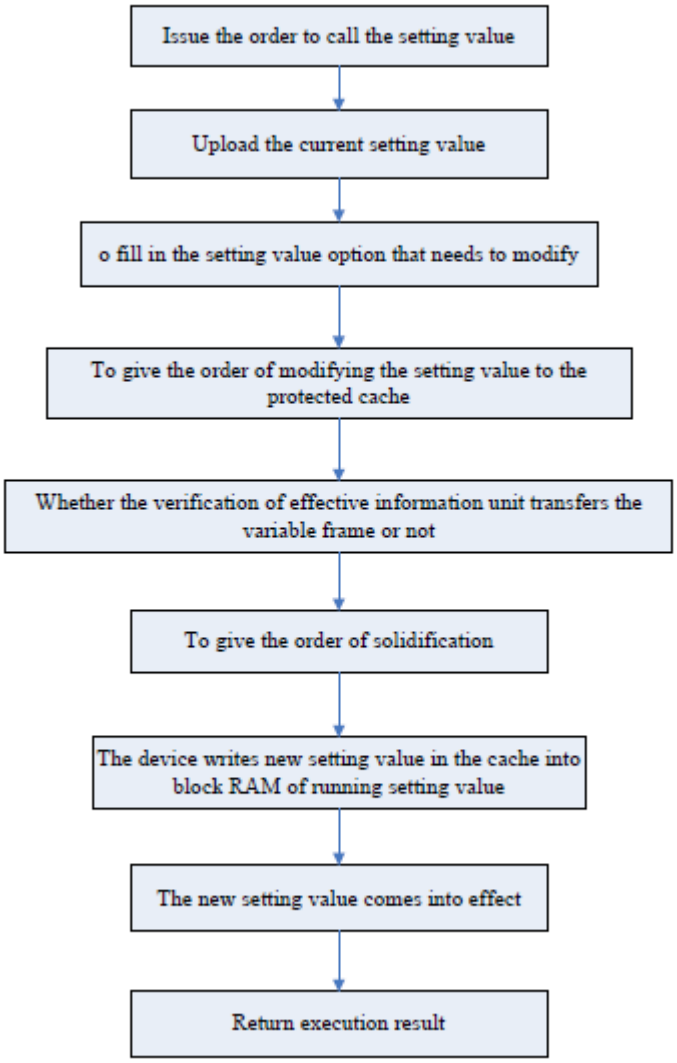


Figure 11: Example of setting modification in micro processing relays (Pingping & Guo 2014)

2.8. Methods for assessing risk for process systems

One method to be considered is Probability Risk Assessment (PRA). PRA is a systematic and comprehensive methodology to evaluate risks associated with every life-cycle aspect of a complex engineered technological entity (e.g. facility, spacecraft, or power plant) from concept definition, through design, construction and operation, and end of life of the equipment (Stamatelatos, 2000). Supporting the PRA are techniques such as event/fault tree analysis and/or cause/consequence diagrams which effectively provide a statement of what events have to conspire together to bring about the undesired outcome (Engineers Australia, 2012).

Fault tree analysis will be useful in identifying the combination of equipment and human failures that can lead to an event and also used to estimate the likelihood of the event occurring. Event tree analysis identifies the range of consequences that a rise from the event and the sequence of events required to produce them (Engineers Australia, 2012). These types of analysis tools will allow the development of a logical view of a risk comparison between the proposed remote management's workflow and the existing workflow providing a clear method of benchmarking between the two.

An important characteristic of many engineering systems is that they behave dynamically. Conventional fault tree methods are designed to illustrate a solid state relationship between logic variables and don't treat dynamic or human behaviours (Siu, 1994). Where the workflows exhibit dynamic behaviours, an extension of the fault tree methods towards explicit state-transition methods (e.g. Explicit Markov chain models) or implicit state-transition methods (e.g. DYLAM) would need to be considered to provide a complete analysis of the risk assessment (Siu, 1994).

2.9. Knowledge Gap

The research has identified there are limited documented applications of remote engineering for protection IEDs. The literature found primarily concentrated on techniques for substation based locations typically on transmission or sub-transmission networks with additional detail around the methods that should be undertaken for on-line management. The research found no documented cases for pole mounted devices and existing practices with Ergon Energy preclude any alternate method for configuration verification for a remote protection setting change.

Owing to little information on power utilities employing on-line techniques to change protection functions of protection IEDs reinforces the need for the project.

2.10. Chapter Summary

Review of relevant standards, regulations and legislation has identified key areas that would need to be considered where any suggested process changes was undertaken. Of note is the draft standard DRAS2067:2014. Although still in draft form, its development by experienced industry professionals would carry considerable weight when comparing any solution.

Limited literature was found on actual occurrence of remote protection IED testing and the information that was available prescribed installation of additional infrastructure (digital simulators) at substations to enable remote protection IED testing.

In regard to alternate methods of configuration verification the review found that there was particular focus on substation environments that are typically part of a transmission and sub-transmission power network. Similar processes for remote testing of isolated/standalone protection IEDs installed in a pole mounted environment to provide a comparison have not been found. This may be owing to other utilities' having a preference of commercial non- disclosure regarding these types of strategies.

The Cigre paper on Remote On-line Management for Protection and Automation provides significant insight into strategies that should be consider for the implementation of a remote management process (CIGRE Working Group B5-09 2006).

Risk assessments will play an important role in understanding the risk for each process. It is proposed initial risk assessments of the existing work flows be subjected to the Probability Risk Assessment (PRA) methodology. If the initial assessment identifies any tasks subjected to dynamic behaviour additional techniques would be needed to complete the risk analysis which could lead to an iterative process as each assessment is developed. Once completed the development of any new process can be benchmarked against the existing process to compare differences and their related impacts.

Chapter 3

Project Methodology

3.1. Chapter Overview

The methodology refers to the approaches that were adopted to successfully achieve the objectives outlined in the project specification outlined in Appendix A. The aim of this chapter is to provide detail on the methods used to successfully address the objectives and provide context to the remaining chapters of the dissertation.

The tasks required to successfully achieve the project outcomes were:

- Research into existing Remote management techniques
- Configuration Management Processes
- Methods of Configuration Verification for Protection IEDs
- Assessment of Remote Configuration Delivery

The following section discusses the methods used to achieve each of these tasks. It should be noted this is not an exhaustive explanation as this is addressed be the remaining chapters of the dissertation.

3.2. Research

The research outcomes have already been discussed in Chapter 2 of the dissertation. The main focus of the research aspect of this dissertation was to identify literature techniques and industry examples that provided further understanding of the challenges

and limitations in developing a remote configuration process that could provide the opportunity to initiate a remote protection setting change of a Protection IED installed on a power utility network.

Considering the project objectives (1), (2) and (3) of Appendix A research in configuration management was undertaken to identify methods to develop a configuration management process. Where possible identifying methods that other power utilities or industry peers were recommending.

Alternate methods for verification of configurations were investigated to enable progression of project objective (4). Literature was reviewed to firstly obtain an understanding of the reasons for existing verification and testing methods and their effectiveness to comply with current legislative, regulatory and power industry standards. This was deemed to be particularly important as the introduction of a remote management process will challenge these methods. Utilities around the world identify similar processes as the next step in developing a smarter and more efficient network with the implementation of such processes scattered across the world and is yet to be embraced on a large scale (Pingping & Guo 2014). Existing verification and testing methods were also examined helping galvanise the project's objective (6) verifying the Protection IED's response to on-line configuration delivery and the operational risks the processes may introduce.

3.3. Configuration Management Processes

The following sections discuss the methods used to fulfil objectives (1), (2) and (3) of the project specification.

3.3.1. Examination of existing practises (Objective 1)

The existing workflow for configuration delivery was analysed to identify root causes of configuration errors. The effectiveness of current management strategies was analysed to determine where improvements could be made. The analysis employed Fault Tree techniques to firstly identify the effectiveness of the current processes and secondly to determine those areas in need for improvement. Two electronic surveys were initiated and distributed to Ergon Energy field test staff to obtain an end user perspective of the existing delivery process. The first captured the perception of the end user's experience with the quality of the delivery and was aimed at identifying any sense of existing

issues. The second survey provided a progressive reporting during the length of the project and was aimed at identifying specific issues with current projects.

The perception survey was designed to capture features of a configuration management process that should be considered in the casual analysis shown in Figure 12 including causes of Protection IED mis-operations described in section 2.5.2.

The 'SurveyMonkey' software package was used to create the questionnaires considering a quality assurance process;

- ***Define*** the problem/s by identify areas for improvement in the current IED configuration delivery
- ***Measure*** configuration discrepancies and their impacts
- ***Analyse*** this information to identify root causes
- Develop and test strategies to ***Improve*** the process
- ***Control*** and support the process through revised documentation

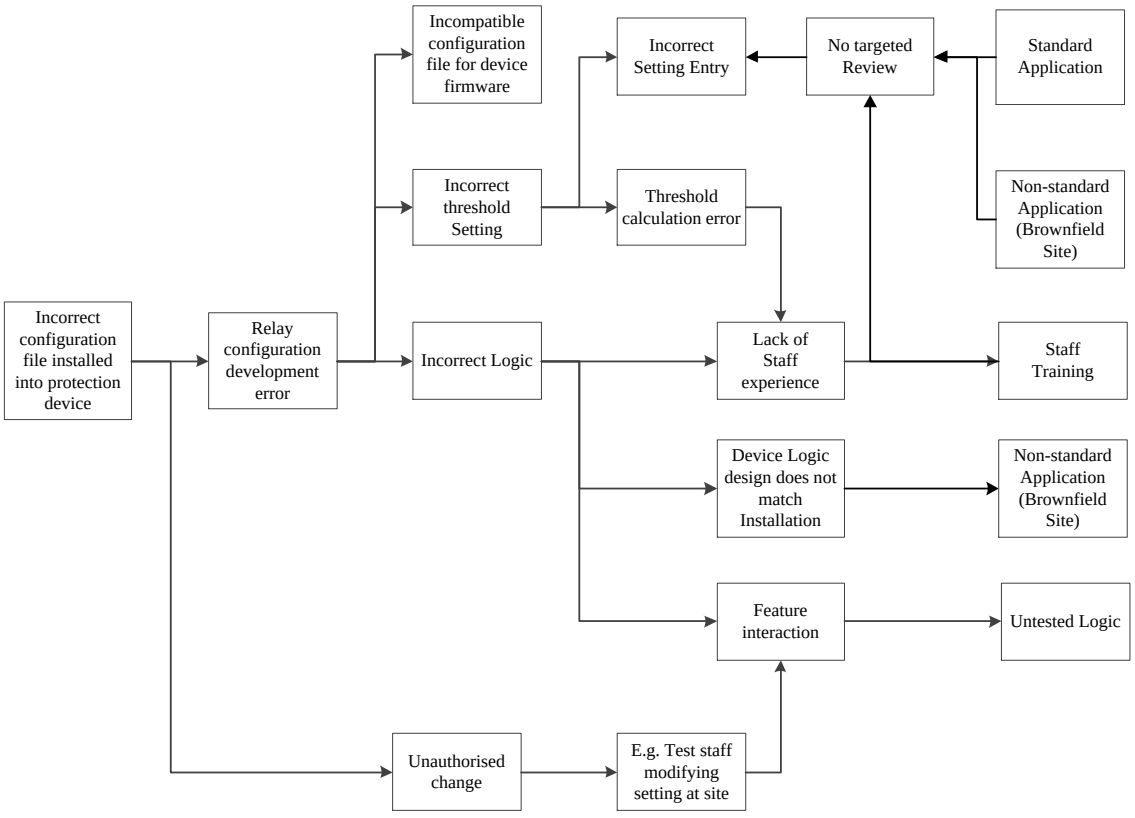


Figure 12: Causal analysis for an incorrect configuration file installed into a protection device.

The perception survey was tested and evaluated for operation and delivered electronically to approximately 95 field test staff. On closure of the survey the results were analysed to identify where the reported errors aligned within the existing workflow. It is acknowledged the perception survey provides a subjective view of the delivery process. Therefore to capture a progressive measure of configuration discrepancies a one page *"Tick and Flick*" repeatable progressive survey was delivered to the same personnel to report on identified errors observed during the present day and over the following 3 – 6 months. The progressive survey provided the ability to compare the results between it and results obtain from the perception survey. It is intended that this survey will be revised and reinitiated at the end of the project to monitor and measure the improvements made to the configuration delivery process.

To obtain endorsement to deliver the survey internally to Ergon Energy presentations to the following stakeholders were undertaken;

1. Ergon Energy's Engineering Standards Management team – This initial presentation was delivered to senior management to firstly obtain approval to issue both surveys and secondly to engage management by providing the opportunity to respond to any concerns and/or offer improvements to the survey delivery.
2. Secondary Systems Managers and Supervisors – To promote the reasons for the survey and to obtain support at the local level to help increase frequency of survey responses.
3. Ergon Energy's Protection team – to inform and advise Ergon Energy's Protection groups of the delivery of each survey and discuss the content of the questionnaire. This was essential owing to the surveys being designed to capture errors of work delivered by these groups.

Owing to the location of staff the presentations were delivered via video and teleconference facilities.

3.3.2. Methods of Setting Verification (Objective 2)

This involved development and examination of methods for setting verification that may be implemented to reduce the likelihood of configuration errors.

To verify a proposed setting has some validity compared to those expected to be applied on the distribution network the possibility of bench marking protection settings was examined. This task initially selected and analysed the subset of settings that were deemed to be most critical for a distribution network. An expectation was that identified techniques may be used to analyse the remaining configuration settings of the Protection IED. The effectiveness of other criteria to capture deviations from previous configuration events such as frequency of change and abnormal increases in setting magnitude were also examined.

3.3.2.1. Bench Marking

The historical settings used for this analysis are located within Ergon Energy's protection database system. To access the required data for the analysis SQL queries needed to be developed to search for each critical setting applied to the basic IED type. The methodology of the initial data for which the SQL script was written to search for is shown in Figure 13.

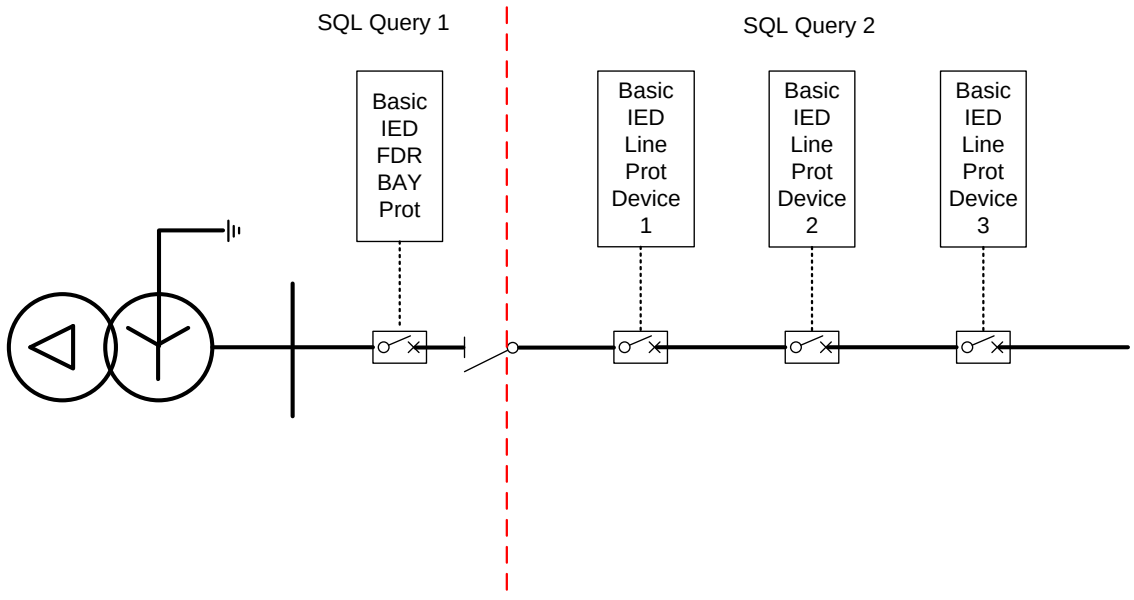


Figure 13: Initial methodology for SQL script development

SQL query 1 was developed to capture all settings of Basic IEDs that have been installed at the substation bay of Ergon Energy 11kV distribution feeders. The second

query (SQL query 2) was developed to capture all settings applied to line devices downstream of the substation. It is suspected for some settings additional queries may be required to provide a more granular approach for a successful analysis. Where considered necessary an example of proposed additional SQL queries are displayed in Figure 14.

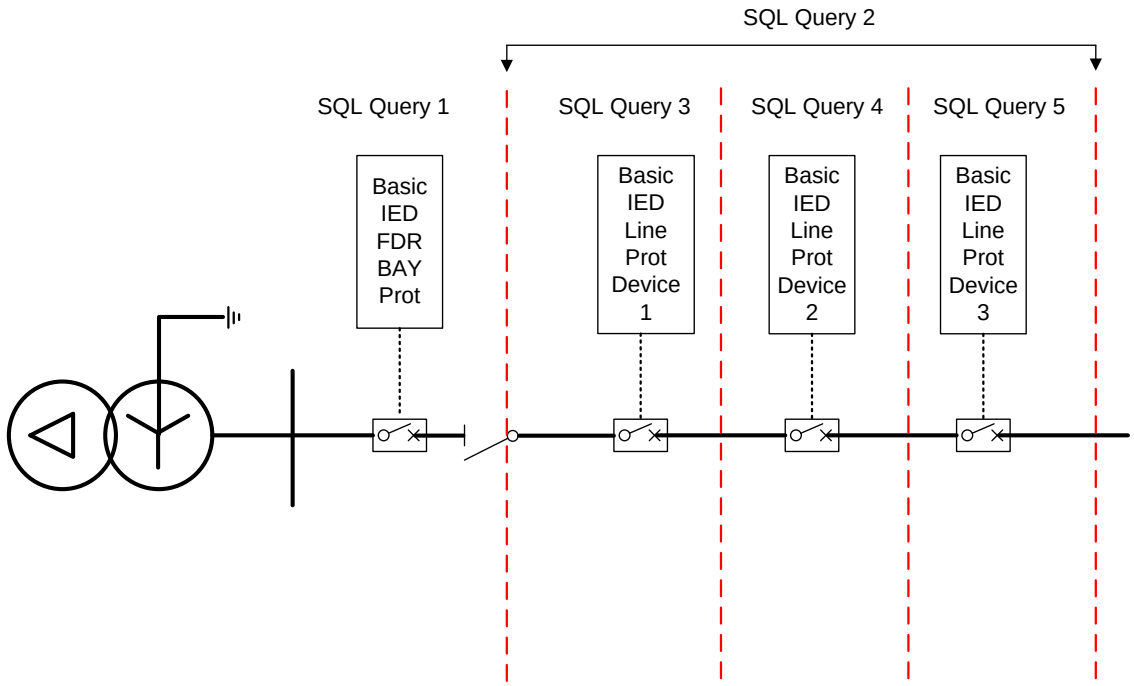


Figure 14: Increased SQL queries for a more granular analysis

3.3.2.2. Measurement of Bench Marking Outcomes

With the data collected it is proposed to expose each setting string to the Normal Distribution functions to determine the mean and standard deviation of each query. The resultant mean and standard deviations are to be analysed against current Ergon Energy protection philosophy to quantify the effectiveness of the analysis. It is hoped this analysis can provide a sanity check of a new proposed setting against historical settings implemented on Ergon Energy's entire distribution network. Furthermore the new setting could employ the following criteria;

- Frequency of change – Flag an abnormality where there is an excessive amount of change to the one setting over a prescribed period of time. This may be indicative of inexperience of the protection setter or an undefined network condition.

- Magnitude of change – Flag an abnormality where there is an increase in magnitude outside a prescribed boundary to capture those settings applied through inexperience.

3.3.3. Development of an Improved Configuration Process (Objective 3)

Development of an improved configuration delivery process was undertaken using the information obtained from sections 3.3.1 and 3.3.2. The survey results provide those areas that warranted the most attention to improve confidence in configuration delivery. It was also important to acknowledge during development of the new process that Ergon Energy's protection schemes still contain a mix of electromechanical, solid state and numerical devices. The project's objectives are centred on Protection IEDs which require configuration files (numerical devices) to deliver the remote management capability. As there still remains a population of electromechanical and solid state protection relays that do not support remote management it was important that implementation of proposed improvements had to ensure no adverse impacts.

3.4. Methods of Configuration Verification (Objective 4)

A review of existing verification techniques used for Protection IEDs was undertaken to identify whether an alternative verification technique could be used to support remote configuration delivery. The proposal is to limit remote management to commissioned devices so remote configuration changes will be initially undertaken on existing Protection IEDs. The analysis was undertaken considering brown field applications (installed devices) for the Basic IED.

With the power utility industry cautious of using alternative techniques to verify installed a review of Ergon Energy's current methods were undertaken by examining the following:

- Case Study – Analyse an abnormality discovered during a recent extraction of a configuration file from a protection device whilst under current verification technique.
- Ergon Energy's standard work practice SP0518 - describing the basic testing philosophies that are currently employed in relation to setting changes to a protection relay.

- National and Queensland regulatory requirements - reviewed to determine the requirements imposed on to Distribution Network Service Providers (DNSP) to remain compliant in relation to protection schemes.

On completion, an alternative processes for remote configuration delivery was developed and is discussed. Highlighting the difference between the software and hardware of a Protection IED is also essential owing to the proposed delivery process eliminating on site testing. To ensure best industry practice is maintained changes to the verification process will be compared to what is currently in use.

3.5. Assessment of Remote Configuration Delivery (Objective 5 & 6)

The following sections introduce the methods used to fulfil objectives (5) and (6) of the project scope.

3.5.1. Simulation of Remote Configuration delivery

Concerns of changing a setting on line during the configuration delivery have been described in section 2.7 (Pingping & Guo 2014). The action of delivering a configuration to a protection IED whilst remaining in service is not common practice for power utilities (CIGRE Working Group B5-09 2006). Therefore it is deemed necessary to test some device types used on Ergon Energy's distribution network to understand the issues associated with this process. The selected device to be tested was one of the Basic type IEDs typically installed on Ergon Energy's 11kV distribution network.

An understanding of how the selected IED should operate during the remote setting delivery process was needed. Owing to manufacturer's intellectual property details of the internal construction and operation of the device is not disclosed publically. The manufacturer was approached to obtain further details and they proceeded to provide a high level description on how the device is expected to respond for configuration delivery whilst in service. A flowchart was developed and provided to the manufacturer

to comment on its accuracy prior to testing. The resultant flow chart from this exercise is shown in Figure 44 section 6.1.1.

To simulate remote configuration delivery to an in service device, a Basic IED located in Townsville was designated as the remote Protection IED. A configuration was sent from a desktop computer located in Toowoomba over the same communication network currently employed to provide engineering access to Protection IEDs shown in Figure 1. Tests were performed under controlled laboratory conditions to assess the accuracy of the flow chart. The tests undertaken for this assessment are described in Chapter 6.

3.5.2. Risk Matrix for Remote Configuration delivery

With the knowledge gained from the literature review, the new configuration delivery process developed, an alternate verification method established and the simulation testing for remote configuration delivery complete, operational risks where determined. These risks were evaluated against Ergon Energy Corporate Risk Assessment Tables evaluating the impact and the control measures that are to be implemented. Furthermore listing recommended considerations in developing checklists for remote configuration delivery capturing the how, what, who, when and why concentrating on the outcomes from section 3.5.1 and recommendations outlined in Clause 6.28, of AS61508.1.

3.6. Chapter Summary

The chapter discusses the processes and techniques used to successfully complete the objectives of the project. Furthermore it provides the opportunity to broadly divide the tasks of the dissertation into; research, configuration management processes, protection IED configuration delivery and assessment of remote configuration delivery. Association of the broad task with each chapter/s is shown in Table 1.

Table 1: Association between the broad tasks, Dissertation chapters and related objectives

Broad task	**Relevant chapters**	**Related objectives**
Research	2. Literature Review	(1), (2), (3), (4), (5)
Configuration Management Processes	4. Protection IED Configuration Management	(1), (2), (3)
Methods of Configuration Verification for protection IEDs	5.Remote Delivery of Protection IED Configurations	(4)
Assessment of Remote Configuration Delivery	6.Response to Remote Reconfiguration	(5)
Risk Matrix	7. Operational Risks	(6)

Chapter 4

Configuration Management

This chapter will identify and assess the existing configuration management processes identifying root causes of configuration errors and suggest improvements to the configuration development process.

4.1. Existing Configuration management practices

To examine Ergon Energy's existing protection configuration delivery process a workflow (Figure 15) was developed with reference to Ergon Energy's P56P02 Protection Setting Procedure document. This identified three key outputs which form part of the configuration delivery.

- The Protection Setting Report
- The configuration file
- The Protection Setting Request (PSR)

The Protection Setting Report is the start of the process. It details the protection setter's method of developing the setting including any network issues that have influenced the final setting or groups of settings to be installed into a protection IED.

The configuration file is vendor specific and is dependent on the intended protection IED. The required settings are applied to a configuration file which is then written to the Protection IED.

The Protection Setting Request (PSR) is a formal document capturing the 'what' and 'where' of the installation; including identifying the Protection IED, thresholds and time characteristics that are to be configured within the Protection IED, and the required

firmware. The PSR is electronically stored and used as the primary reference document for Ergon Energy operational staff.

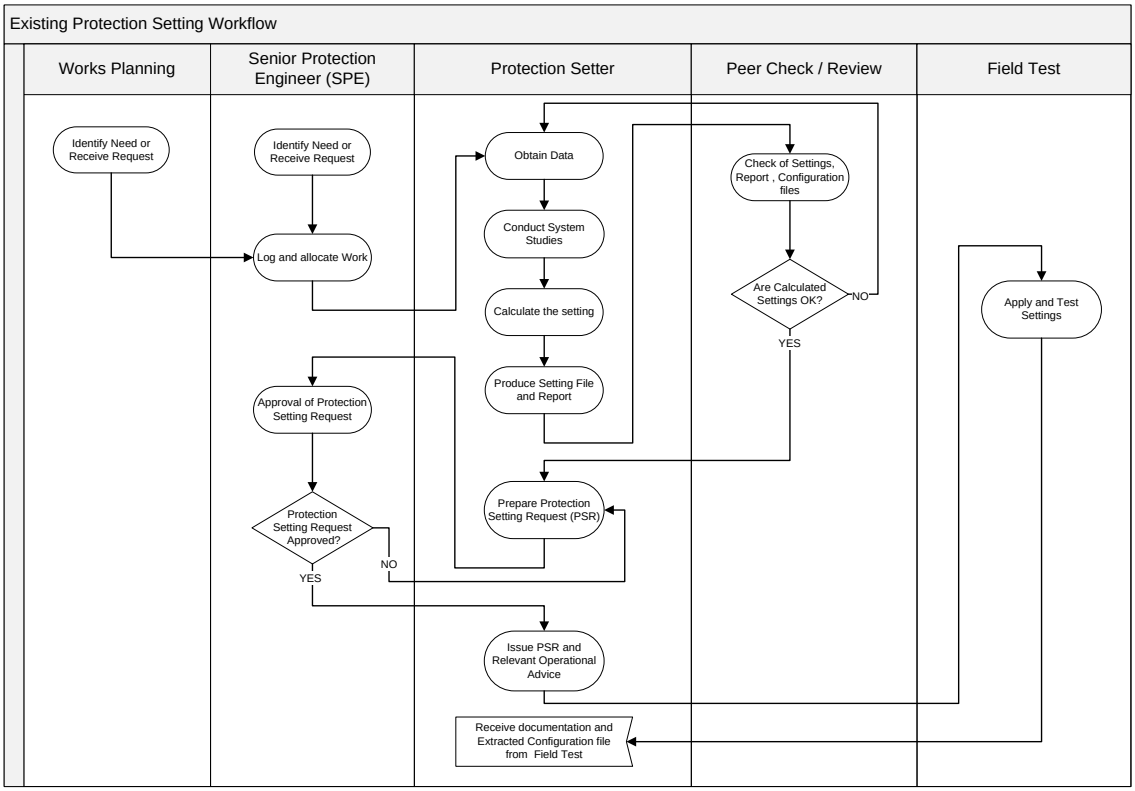


Figure 15: Existing Protection Setting Workflow

To examine the effectiveness of the existing configuration delivery process a fault tree analysis was undertaken for the development of settings for non-standard and standard applications providing an estimated probability of error.

Figure 16 identifies the probability of error for Non-Standard (Brown field) application and Figure 17 provides the probability for Standard applications. Each task within the fault tree was assigned a probability of occurrence dependant on its perceived activity type (Engineering Australia 2012). The values used are listed in Appendix B. The probability values used during the fault trees analysis considered the worst case scenario where the protection setter was deemed to be less experienced in the development of the Protection Setting report and configuration of the Protection IED. Where these tasks were performed by a more experienced protection setter then the probability of error is expected to be lower.

4.1.1. Non-Standard Configuration delivery

Four milestones were identified within the fault tree analysis aligning to the outputs provided by the protection setter;

- Error in Protection Setting Report
- Configuration file error
- Protection Setting Request (PSR) error
- Error in configuration delivery

Setting report errors are influenced by calculations and changes to control functions and logic to support non-standard installations. Based on the fact that the primary focus of the protection setter is to protect the network, errors in thresholds and or time characteristic were deemed as routine tasks that would require some care. Non-standard applications typically include changes to input and output logic, control and SCADA indications for specific application. These works were deemed to be complicated non-routine tasks owing to the deviation from what the setter would be accustomed to. Issue of the Protection Setting Report would occur after peer review. The probability of error applied here is that of a walk around inspection owing to the fact that there is no defined description of the targeted features that should be reviewed.

Configuration file error is influenced by the setter's knowledge and experience with the Protection IED when applying features that deviate from a prescribed standard.

Applications of standard features to the logic would have low probability of error; however the application of non-standard logic may create feature interaction or be simply entered incorrectly. The Protection Setting Request (PSR) is derived from either the Protection Setting Report or by the configuration file. This depends on the how the setter steps through the process. Method 1 (displayed is Figure 16) where the setter has created the Protection Setting Request (PSR) directly from the Protection Setting Report. Method 2 (displayed in Figure 17) is where the setter has used the configuration file to create the Protection Setting Request (PSR).

Ultimately an error in the configuration delivery is managed by both the peer review employed to detect errors generated within the configuration file and the method of error generation within the Protection Setting Report.

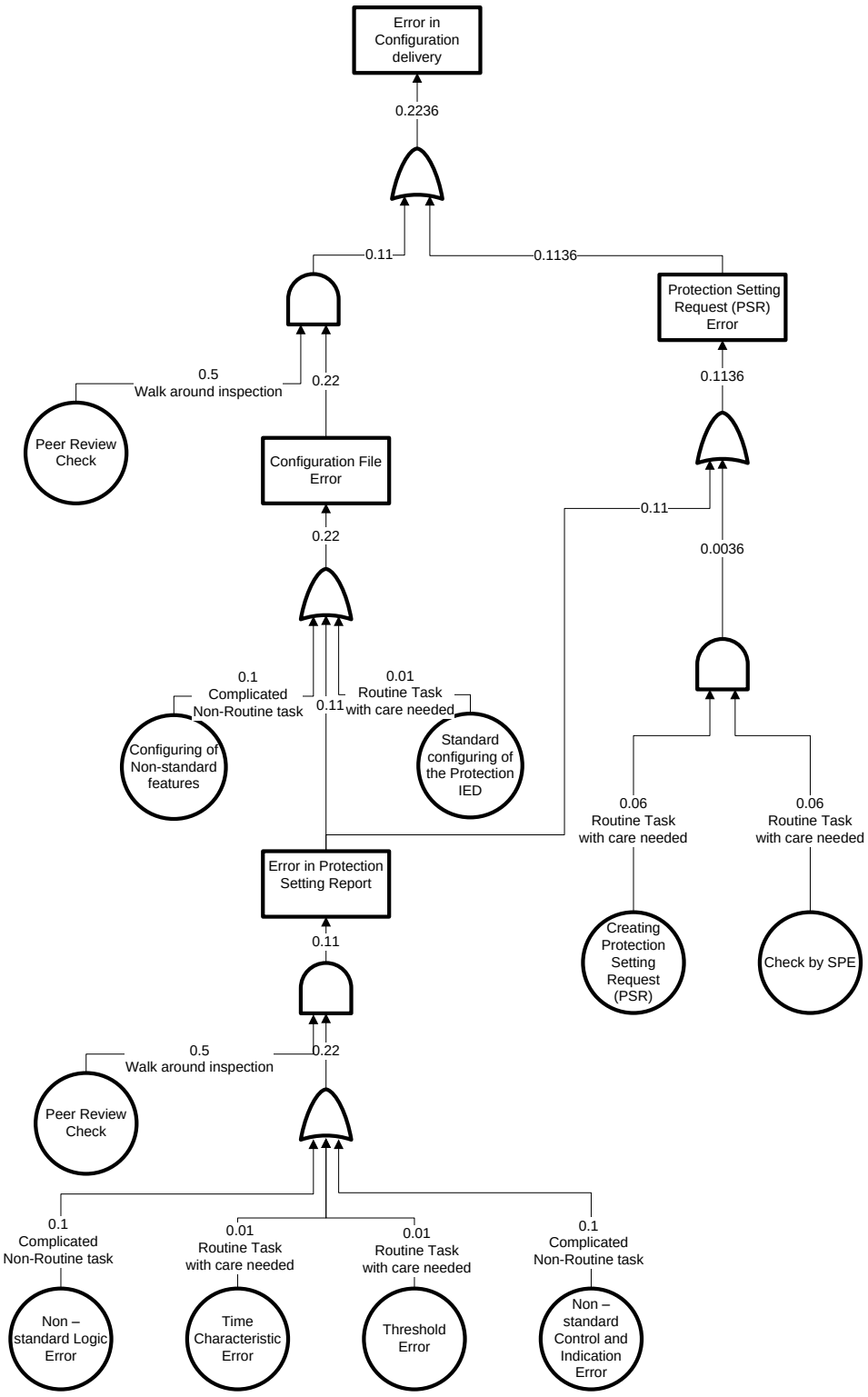


Figure 16: Fault tree for Non-Standard configuration delivery (method 1)

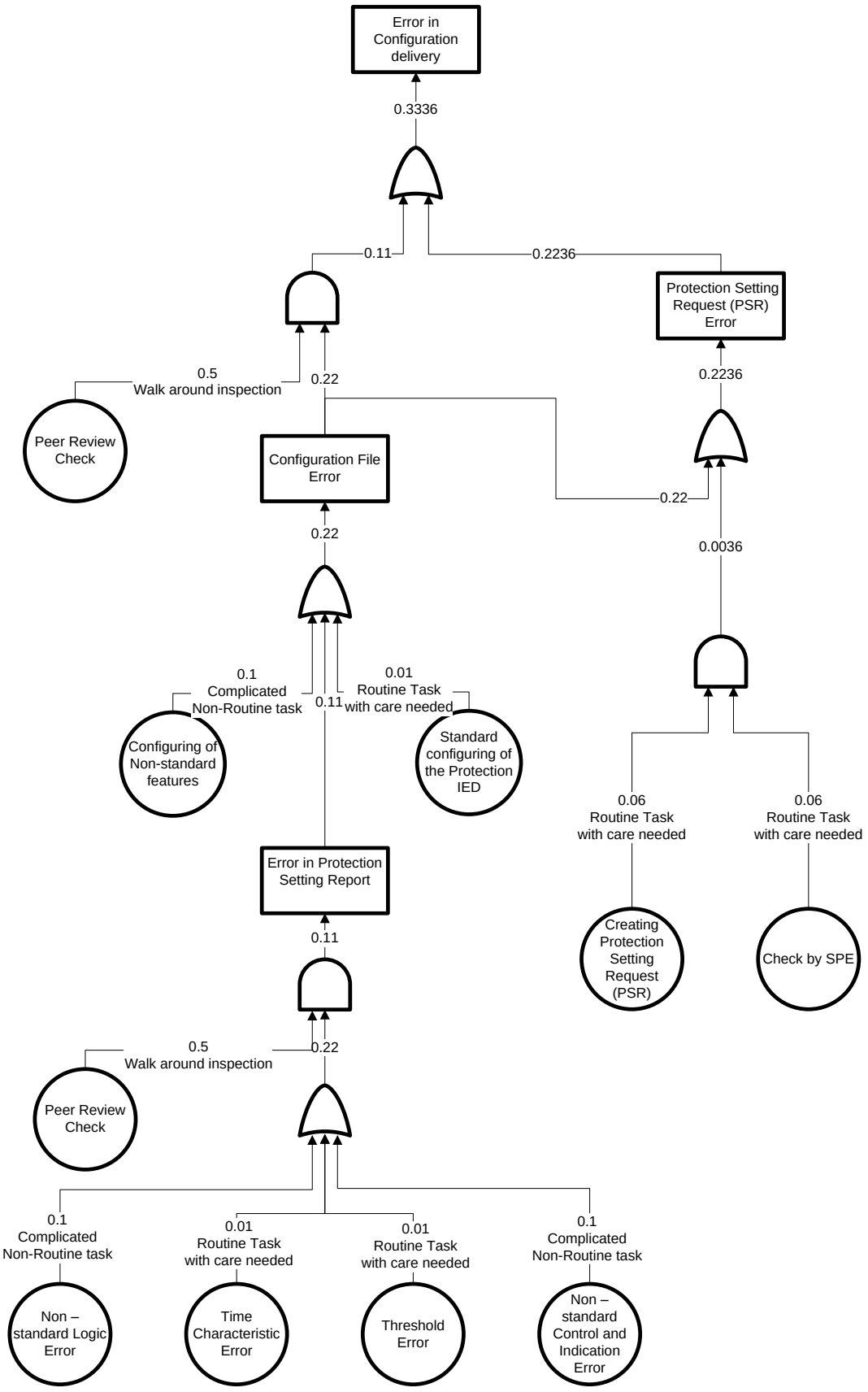


Figure 17: Fault tree for Non-Standard configuration delivery (method 2)

4.1.2. Standard configuration delivery

The same four milestones were identified within the standard configuration delivery fault tree analysis, once again aligning to the outputs provided by the protection setter;

- Error in Protection Setting Report
- Configuration file error
- Protection Setting Request (PSR) error
- Error in configuration delivery

The same error probabilities are used as expected in the non-standard application, however for standard applications the non-routine tasks are not present as these have already been accounted for. Changes to input and output logic, control and SCADA indications were not considered owing to standard configurations contain pre-defined descriptions regarding these features. Setting report errors are influenced by calculations for the desired application. Checking of the report is similar to a walk around inspection owing to there is no defined description of the targeted features that should be reviewed.

Configuration file errors are limited as the setter's knowledge and experience with the Protection IED is only required to apply trip thresholds and time characteristics, which is deemed to be a routine task with care needed.

The Protection Setting Request (PSR) is influenced by either the Protection Setting Report or by the configuration file. This depends on the how the setter steps through the process. Figure 18 displays method 1 where the setter has created the Protection Setting Request (PSR) directly from the Protection Setting Report. Figure 19 displays method 2 where the setter has used the configuration file to create the Protection Setting Request (PSR).

Errors in configuration delivery are managed by peer review employed to detect errors generated within the configuration file and method of error generation within Protection Setting Report.

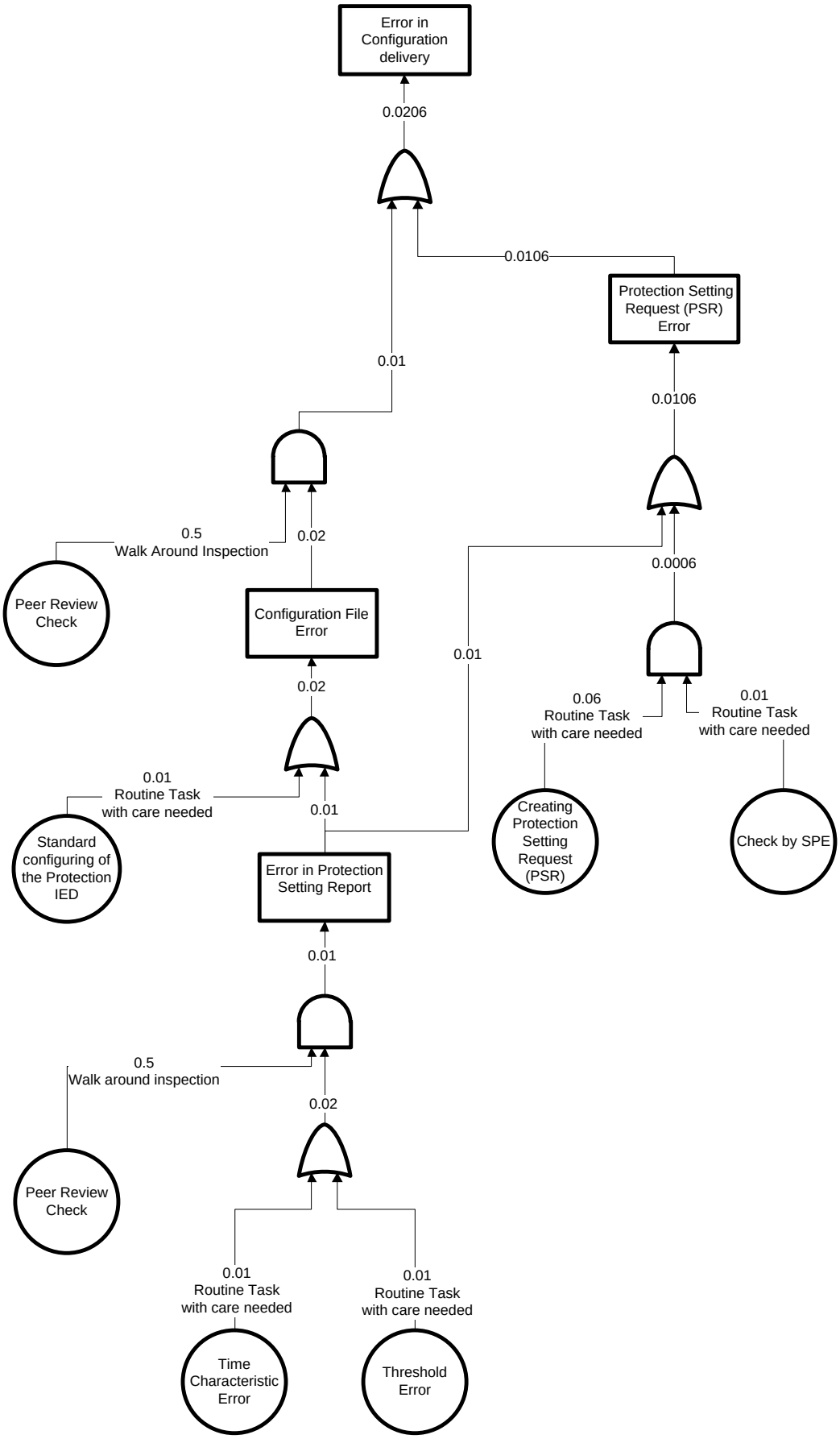


Figure 18: Fault tree for Standard configuration delivery (method 1)

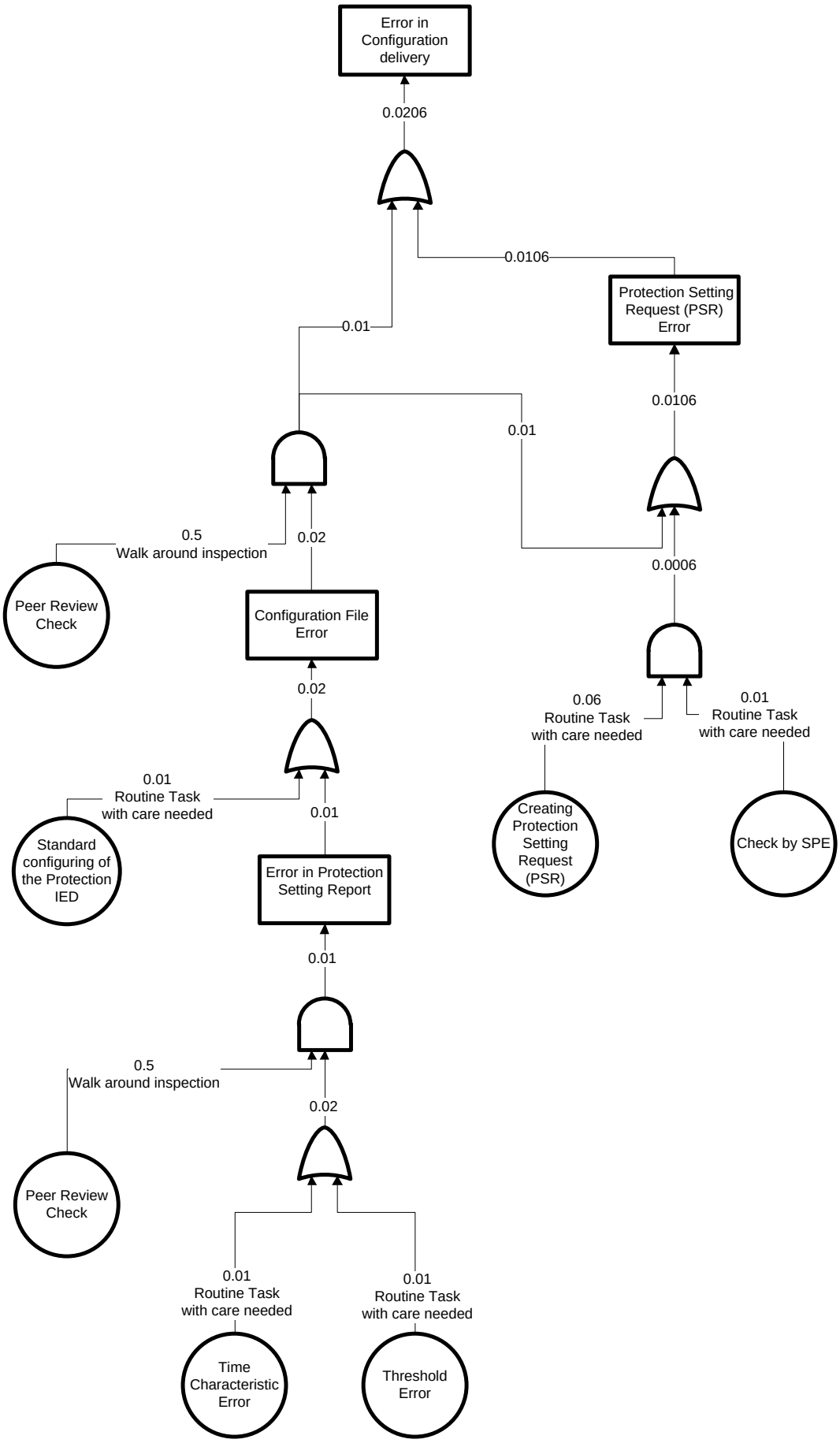


Figure 19: Fault tree for Standard configuration delivery (method 2)

4.1.3. Results of fault tree analysis

Each of the non-standard and standard processes were examined considering their associated milestones. The decision for the setter to choose one or the other direction through the process for the non-standard delivery produced different ranges of probability error ranging from 22.36 % to 33.36%. The standard delivery was not affected by the differing paths through the process providing probability error of 2.06%

4.2. Effectiveness of existing Configuration Management Practices

The effectiveness of the existing practices was captured by the use of perception and progressive surveys.

4.2.1. Perception survey results

The perception survey described in section 3.3.1 was delivered to 97 field test staff and returned a response of approximately 38% of the total number. This was due to the fact that it was a voluntary survey and that some staff had not been exposed to the device types covered by the survey. The data collated provided an indication of where to investigate to improve the existing workflow.

The perception survey targeted both commissioning and operational configuration changes. Average errors rates for commissioning and maintenance were 35% and 22% respectively and are displayed in Figure 20 and Figure 21. Commissioning was deemed to be where a setting or configuration was issued for a new installation and operational changes covered existing installations that required changes due to feeder augmentation works or responses to protection feeder reviews. The survey questions developed to obtain these results are provided in Appendix C.2. A CIGRE paper on fault statics for Protection IED lists the error rate for numerical protection relays undergoing commissioning tests at 35% (Kjolle 2002); indicating the results from the perception survey may not be unrealistic.

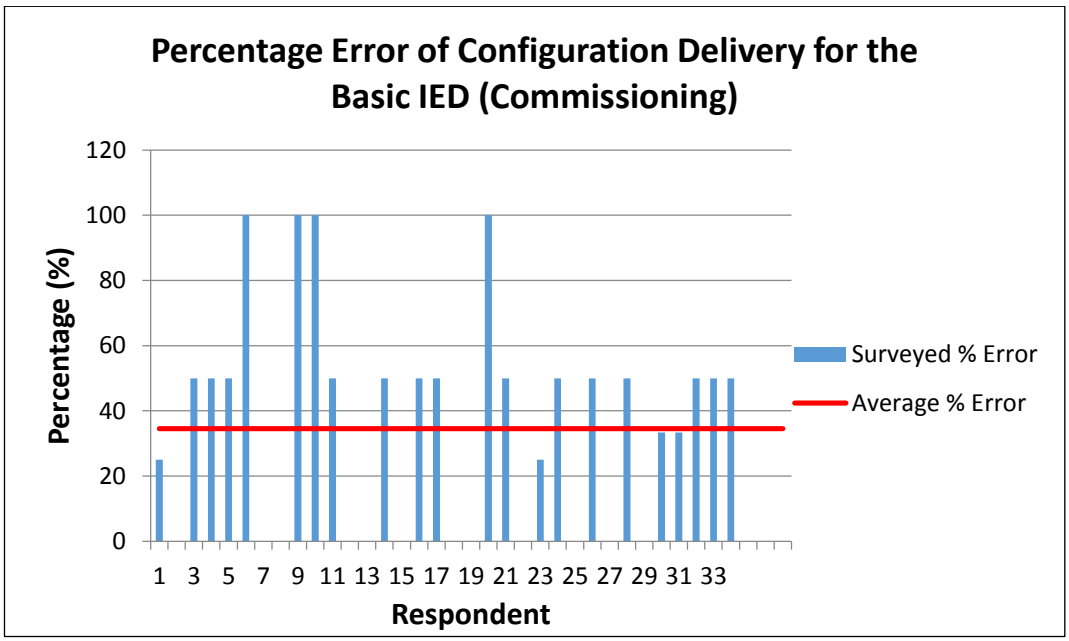


Figure 20: Surveyed percentage error of configuration delivery for the Basic IEDs (Commissioning)

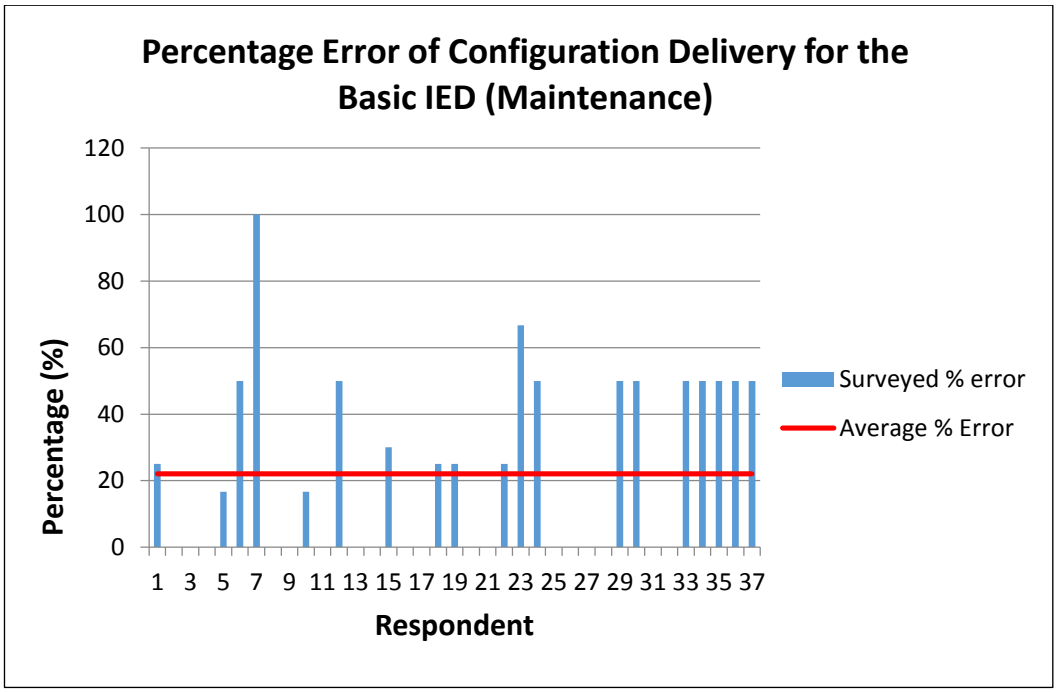


Figure 21: Surveyed percentage error of configuration delivery for the Basic IEDs (Maintenance)

On acknowledging an error the respondents were then progressed through the perception survey and asked to rank the occurrence of errors of key features that were deemed operational critical for the Basic IED. These features were chosen on industry experience and considering the mis-operation literature discussed in section 2.5.2; these

features included Tripping thresholds, Time characteristics, Control and Indication and Device firmware with the results shown in Figure 22.

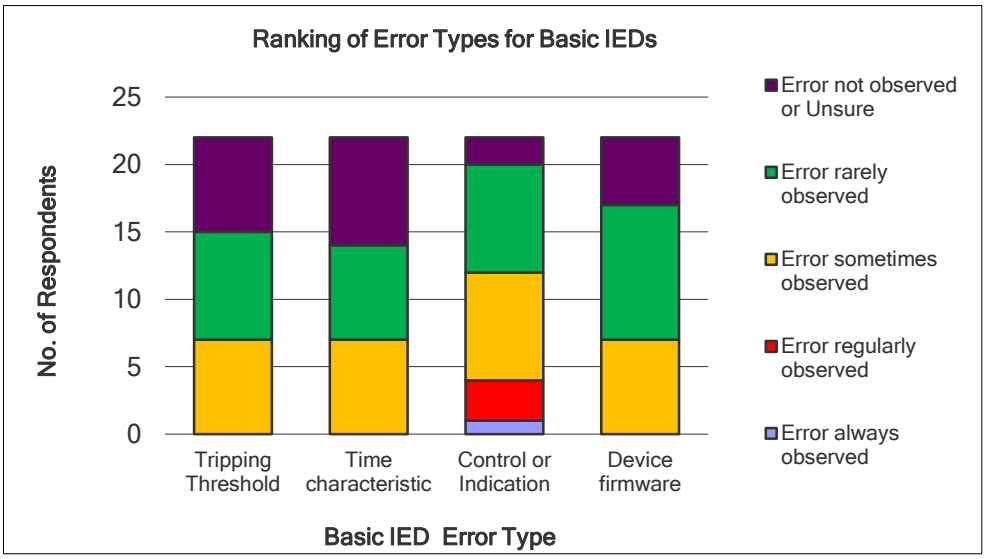


Figure 22: Perception survey - Ranking of error types for Basic IEDs

This initial ranking of the key components shown in Figure 22, identified that each were subjected to an error when delivered to the end user. Tripping and time characteristics were ranked similar, with 2% of the responses acknowledging errors are sometimes observed. Control and indication responses returned a combination of observations, 4% were errors always observed, 9% were regularly observed and 36% of responses were error sometimes observed. Finally the result for device firmware indicated 27% of the responses sometimes observed the error.

Tripping and time characteristics were of some concern prompting further examination into the reasons for this discrepancy. Over 50% of responses consistently had errors in control and indication, highlighting a high deficiency in the existing Protection Setting workflow. The results reported 27% of responses identified device firmware to have an error sometimes observed. Ergon Energy has gone to great lengths to manage firmware and vendor software for of all protection IEDs. This response was an interesting and unexpected result.

To help further examine these results the perception survey questions were designed to identify the origin of the discrepancies. Where the respondents had identified a discrepancy of one or more of these features displayed in Figure 22, they were asked to

rank the origin and type of error to help further identify root causes of error within the configuration delivery workflow. The results of these more granular questions are provided in Appendix C.3. The origin of the error is summarised in Table 2 which lists the three key documents that are developed and issued to deliver a configuration file for a proposed Protection IED. The results for the 'type of errors' have been used as areas of concentration in developing improvements to work flow outlined section 4.4.

Table 2: Survey question summary for the origin of errors for the Basic IED

Basic IED Features	**Origin of the Error**		
	Protection Setting Report	**Protection Setting Request (PSR)**	**Configuration File**
Tripping Threshold	High	Medium	Low
Time Characteristics	High	Medium	Low
Control or Indication	High	N/A	Medium
Firmware	N/A	High	Low

4.2.1.1. Summary of Perception survey

Table 3 indicated the highest origin of error experienced by field test staff was the protection setting report, followed by the PSR, then by the configuration file. It must be acknowledged that the discrepancies provided by this survey do not in away reflect the validity of the setting to detect network faults. The results only highlight that the end user identifies discrepancies between the three components of the delivery process used to install the required setting. Standard Work Practice (SWP) SP0518 (Ergon Energy 2012) directs test staff to compare these documents to ensure they align with each other prior to testing Protection IED. An example identified is where a Protection Setting

Report requests a setting of 60A and the nearest available setting selected in the device is 58A. According to the testing SWP this would be classified as an error and most likely it would be attributed to the report.

4.2.2. Progressive Survey

The progressive survey which continued to run over the length of the project targeting key error types in Figure 22 as well as capturing functional logic and design. The addition of logic and design was included to capture errors associated with the higher level device types (intermediate and integrated IEDs) to help progress remote configuration for these Protection IED types in the future. It was also deemed prudent for this information to be included into any improvements made to the existing configuration development workflow. The responses obtained by the progressive survey are displayed in Figure 23.

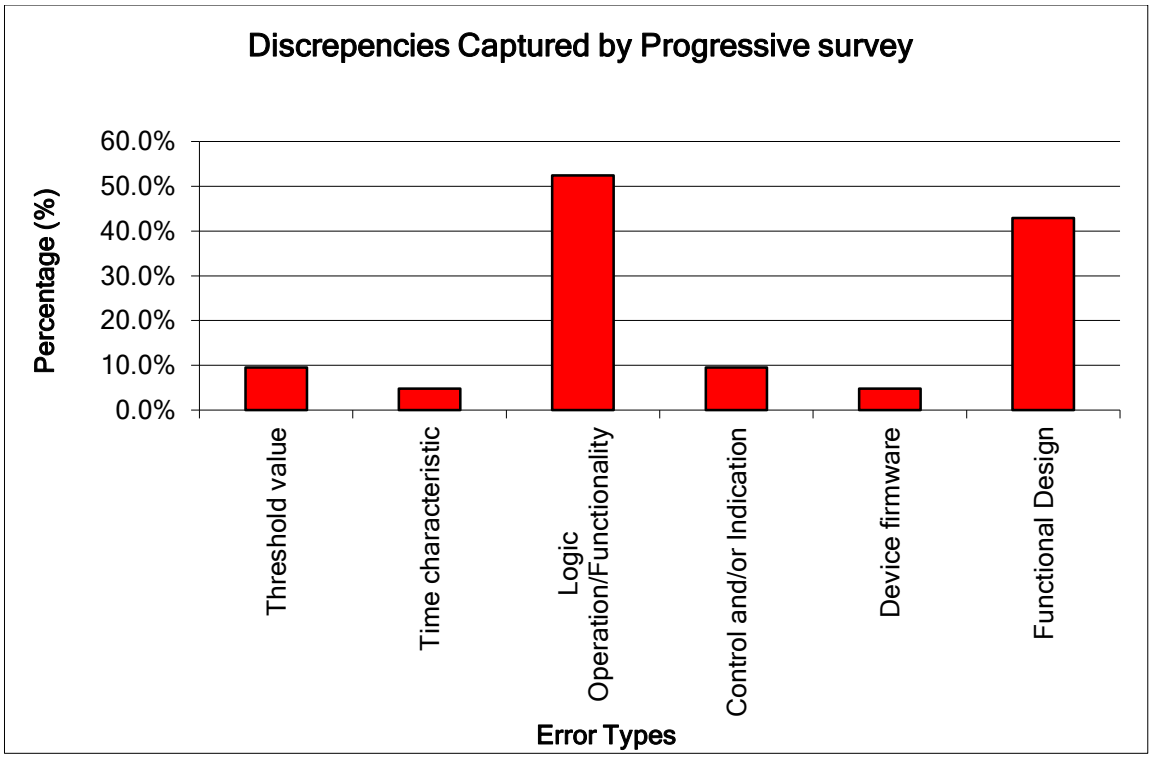


Figure 23: Error types identified by the Progressive survey

4.2.2.1. Results of the Progressive survey

The progressive survey confirmed each of the aforementioned outputs remain susceptible to errors under the existing configuration workflow. With tripping and timer characteristics returning a 10% and 5% discrepancy rate respectively. This was an improvement compared to the original result obtained by the perception survey. Device firmware was also lower at a value of 5%.

The components of functional logic and design added to the progressive survey provided valuable information for the reasons for functional logic errors. Surveying these components returned a 51% error rate for functional logic, and an error rate of 41% for functional design. As these two components are interrelated to obtain correct functionality the error rate returned would suggest for some of these errors there is a direct relationship between the two components. Where a design of the installation varies to the configured functional logic of the Protection IED the end user may interrupt this as a configuration error. Under these circumstances the error is not with the workflow but with the information provided prior to configuration development.

These results to date have only captured errors related with the configuration delivery of the intermediate protection IEDs owing to the lack of Basic IEDs installed over the time of the progressive survey. The workflow under examination is used to develop and deliver configuration files and documentation for both Basic and Intermediate Protection IEDs, therefore these results thus far provide an actual insight into the effectiveness of the existing workflow. Once the recommended improvements have been implemented the progressive survey will be continual improved to remain as an active tool to help further measure, analyse and develop improvements to the configuration workflow.

4.3. Methods of Setting Verification

The survey response indicated that the Protection setting report was a component of the delivery process that needed improvement. The following sections investigated some potential methods of verifying critical settings that are developed and captured within the setting report. To analysis the effectiveness of these proposed methods selected critical settings for the Basic IED were identified and used for the analysis.

4.3.1. Critical Settings for a Distribution Network

Table 3 lists those settings that were deemed most critical and those that were data mined within Ergon Energy's Protection Database System by using the first SQL query as described in section 3.3.2.1.

Table 3: Critical settings for a distribution network

Protection Element	Application
Overcurrent	• Overcurrent protection is designed to detect and isolate for short circuits between two or more phases.
Earth Fault	• Earth fault protection is designed to detect and isolate for short circuits between a phase and neutral or a phase and earth.
Sensitive Earth Fault (SEF)	• Sensitive Earth Fault protection designed to detect and isolate those faults that are beyond the sensitivity of the IDMT Earth Fault protection elements.
Phase time multiplier	• Increases the phase overcurrent setting and typically is set to a multiple of 1.0 times the applied overcurrent threshold.

4.3.2. Criteria of selected settings

To analyse the results of the SQL query an understanding of Ergon Energy's requirements for determining appropriate setting for each of the critical settings listed in Table 3 was needed. The Ergon Energy standard document STNW1002 (Ergon Energy 2014) lists the recommended criteria for overcurrent, earth fault and sensitive earth fault thresholds when determining an appropriate setting for an intended application.

One of the most critical criteria in determining tripping thresholds for each setting is to ensure detection of all possible faults located within the protected zone. The ability for a protection device to detect these is commonly referred to as the Protection Reach Factor (also known as Safety Factor, Operating Reach Factor or Reach). The Protection Reach Factor applies to both the overcurrent and earth fault settings; and can be defined as the

ration of the minimum fault current of a protected zone divided by the pickup setting of the upstream primary protective device (Ergon Energy 2014).

$$\text{Protection Reach Factor} = \frac{I_{fmin}}{I_{pickup}} \qquad (4.1)^3$$

Where:

- I_{fmin} – minimum fault current in the protected zone
- I_{pickup} – the setting threshold of the protection element

Calculation of these reach factors are typically performed using modelling tools. It is important to acknowledge the variables and methods that are used to determine the minimum Protection Reach Factors for applied overcurrent and earth fault thresholds to provide validation of the results produced by first SQL query described in section 3.3.2.1.

The Ergon Energy standard STNW1002 describes Protection Reach Factors for both Primary and Backup applications. Primary protection is considered as the device directly upstream of the fault location and is expected to detect the fault in the first instance. In cases where the primary device fails to operate the next upstream device is configured to provide backup. This philosophy complies with the National Electricity Rules requirement for credible contingencies for fault clearance (AEMC - Australian Energy Market Corporation 2014).

4.3.2.1. Overcurrent Protection Reach Factors

The prescribed Protection Reach Factors for overcurrent thresholds are listed in Table 4. Phase multiplier is also considered in regard to the reach factors as application increases the pickup setting (I_{pickup}) by the multiple of Phase multiplier.

[3] (Ergon Energy 2014)

$$\text{Protection Reach Factor} = \frac{I_{fmin}}{I_{pickup} \times \text{Phase Multiplier}} \quad (4.2)$$

Table 4: Overcurrent Protection Reach Factors

Protection Reach Factors / [Minimum]	System Normal	Abnormal Network Operating Condition
Primary Protection	1.7	1.3
Backup Protection	1.3	1.3

4.3.2.2. Variables determining Overcurrent Protection Reach Factors

A simplified circuit for a phase to phase fault on a distribution network is shown in Figure 24. The circuit identifies the variables that determine the magnitude of phase to phase fault current (If) produced. To calculate the prospective phase to phase fault that the protected equipment or line is subjected to and an equivalent sequence component circuit shown in Figure 25.

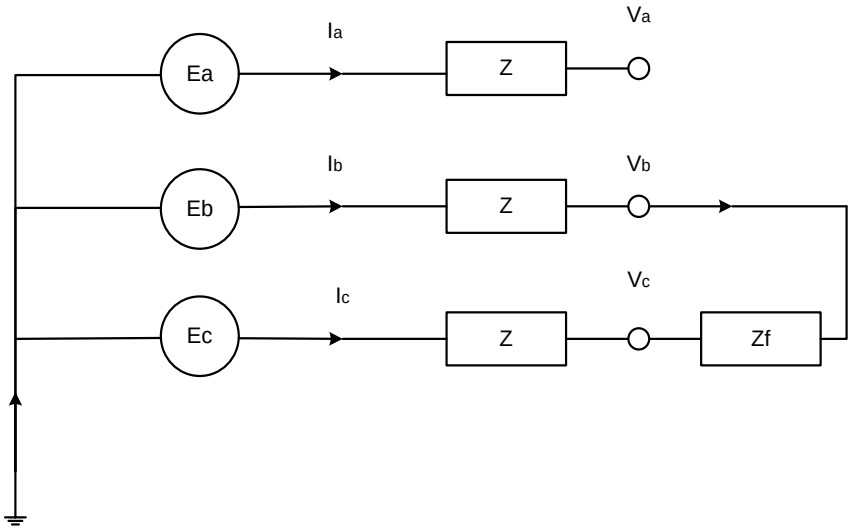


Figure 24: Simplified Impedance circuit for a phase to phase fault

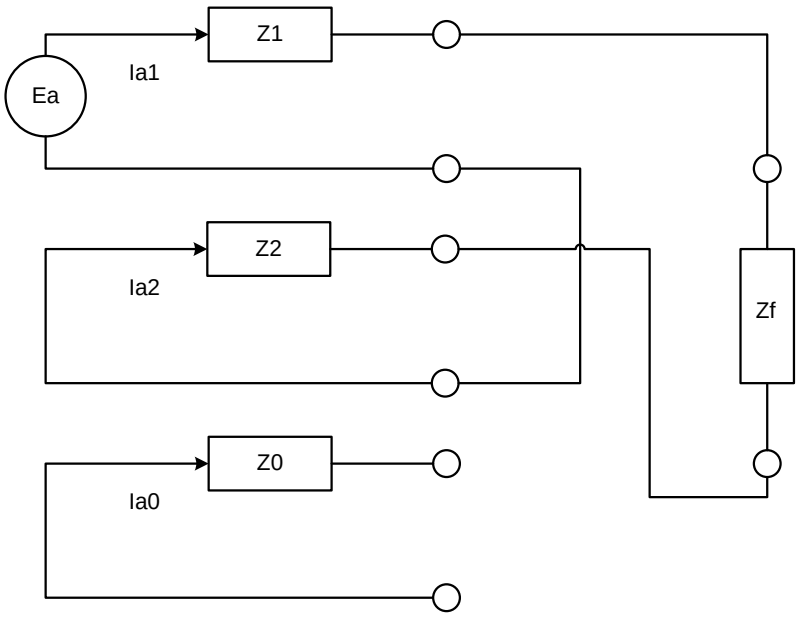


Figure 25: Sequence component connection for a phase to phase fault

These equivalent sequence components are then used to determine the phase to phase fault current detected on the network by the following formula;

$$I_{a1} = -I_{a2} = \frac{\mathrm{E_a}}{\mathrm{Z_1 + Z_2 + Z_f}} \tag{4.3}$$

Where:

I_{a1} – is the positive sequence current

I_{a2} – is the negative sequence current

$\mathrm{E_a}$ – is the source voltage

$\mathrm{Z_1}$ – is the positive sequence impedance

$\mathrm{Z_2}$ – is the negative sequence impedance

$\mathrm{Z_f}$ – is the fault impedance

The $\mathrm{Z_f}$ of the circuit shown in Figure 25 is typically assumed to be of low impedance value for phase to phase faults. Owing to the low fault impedance the magnitude of

fault current calculated would mainly be dependent on the sequence positive (Z1) and negative (Z2) impedance. Typically for non-rotating plant and where the fault location is remote from generation Z2 is assumed to be the same as Z1. These impedances values on a distribution network vary depending on the strength of the source and the conductor impedances of the network. These impedances determine the level of fault current that is presented to the Protection IED. The protection setter uses these values in conjunction with the overcurrent Protection Reach Factors given Table 4 to obtain the required tripping threshold. Overcurrent tripping thresholds therefore vary depending on the networks topology, conductor sizes and lengths.

4.3.2.3. Earth Fault Protection Reach Factors

The prescribed Protection Reach Factors for Earth Fault thresholds are listed in Table 5.

Table 5: Earth Fault Protection Reach Factors

Protection Reach Factors / [Minimum]	System Normal	Abnormal Network Operating Condition
Primary Protection	2.0	1.3
Backup Protection	1.3	1.3

4.3.2.4. Variables determining Earth Fault Protection Reach Factors

A simplified circuit for a phase to earth fault on the network is shown in Figure 26. The circuit identifies the variables that determine the magnitude of phase to earth fault current (If) produced. To calculate the prospective phase to earth fault current that the faulted equipment or line is subjected to an equivalent sequence component circuit as shown in Figure 27.

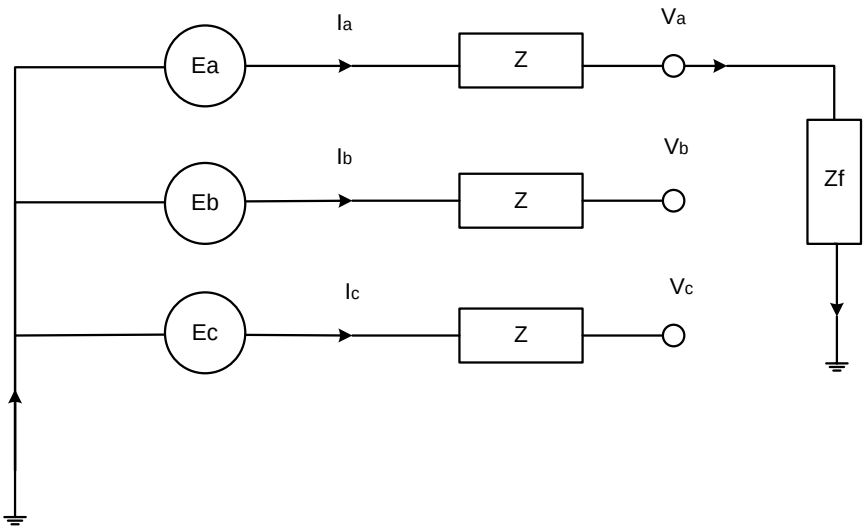


Figure 26: Simplified impedance circuit for a phase to neutral / ground fault

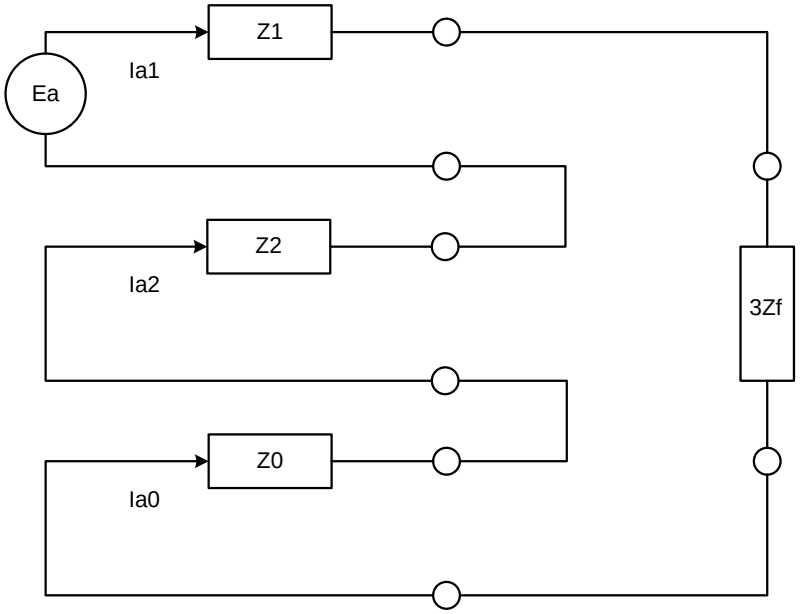


Figure 27: Sequence component connection for a phase to neutral / ground fault

The equivalent sequence impedances are used to determine the phase to ground fault current detected for the network using the following formula;

$$I_{a1} = \frac{\mathrm{E_a}}{\mathrm{Z_0} + \mathrm{Z_1} + \mathrm{Z_2} + 3{\cdot}\mathrm{Z_f}} = I_{a0} = I_{a2}$$

(4.4)

Where:

I_{a1} – is the positive sequence current

I_{a2} – is the negative sequence current

I_{a0} – is the zero sequence current

E_a – is the source voltage

Z_1 – is the positive sequence impedance

Z_2 – is the negative sequence impedance

Z_f – is the fault impedance

Ergon Energy's present protection philosophy sets the Z_f in Figure 27 to a value of 50Ω for earth fault analysis. This is significantly higher than the combined source and line impedances of the upstream network providing a relatively consistent value of impedance for the protection setter to use in conjunction with the earth fault Protection Reach Factors (given in Table 5).

4.3.2.5. Sensitive Earth Fault Protection

Sensitive Earth Fault thresholds are typically set to as low as possible. Due to imbalance on the distribution network the recommended minimum setting is 3A with a definite time of 3 seconds (Ergon Energy 2014). Sensitive Earth Fault settings are typically time and current graded with upstream devices. To accommodate, Sensitive Earth fault settings are recommended to start at 8A, 8 seconds at the start of the feeder (Zone substation) and reduce by 1A and 1 second progressively on any associated downstream devices; an example of this method is shown in Figure 28.

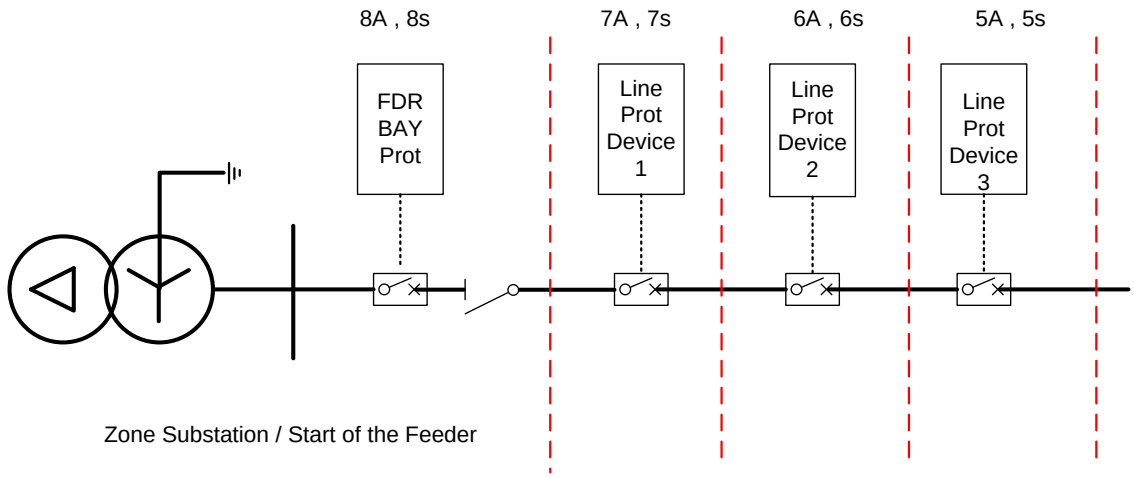


Figure 28: Example of Sensitive Earth Fault coordination

4.3.3. Benchmarking Settings

The following sections discuss the results obtained from the SQL queries to examine the possibility of benchmarking proposed settings.

4.3.3.1. Benchmarking Overcurrent Thresholds

The result of the SQL query 1 for the outgoing overcurrent is shown in Figure 29. It is evident by the graph that the tripping thresholds range is diverse in value and frequency. An excursion of a predefined number of standard deviations from the mean would not be indicative of an appropriate threshold. The use of this method to provide a bench mark or indicator was found to be inappropriate for the protection setter or checker to deem the proposed setting to be correct.

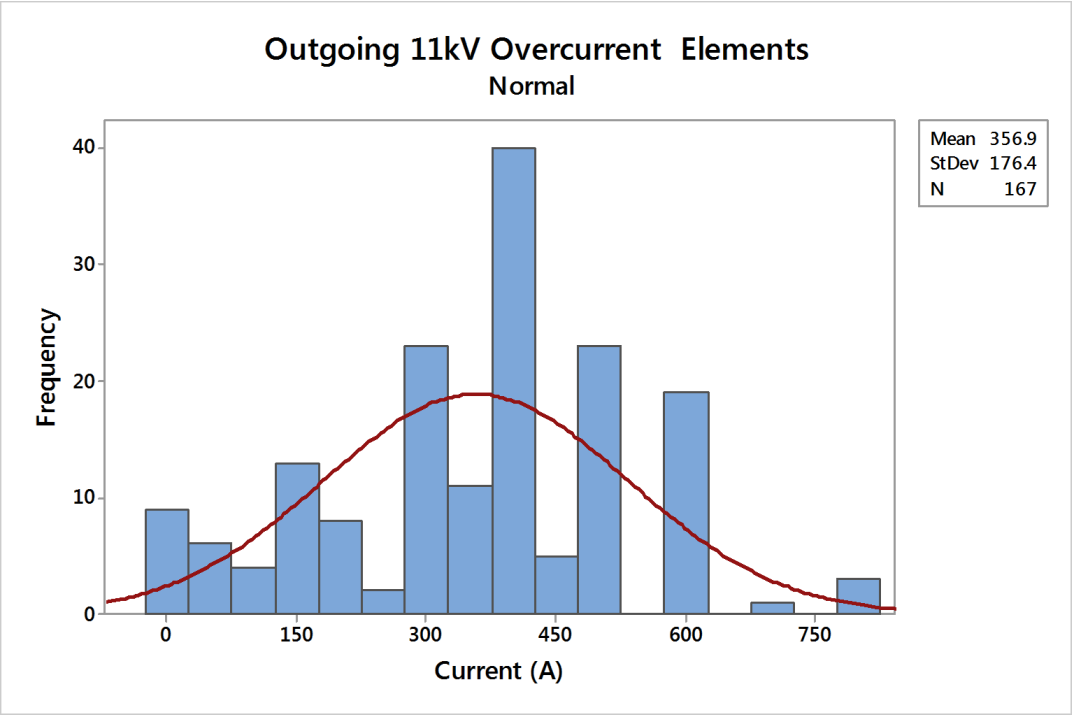


Figure 29: Distribution of Outgoing 11kV Overcurrent tripping thresholds (SQL Query 1)

The result obtained from SQL query 2 for all overcurrent pickups downstream of the feeder bay are shown in Figure 30. This returned a skewed distribution of values which is indicative to the design or application required by these devices i.e installed where protection reach factors are compromised and a line recloser has been installed to provide appropriate detection which inturn typically results in a small value of threshold magnitude. Similar to the outgoing 11kV anlysis a protection setter or checker could not rely on this graph to confirm correctness of the setting however the graph can provide an indication of settings that are outside what is typically applied. The example of this is the red circled setting (900A) in Figure 30. This setting may be appropriate but the method provided the ability to flag to the Protection Engineering Manager to investigate the reasons for such a large setting.

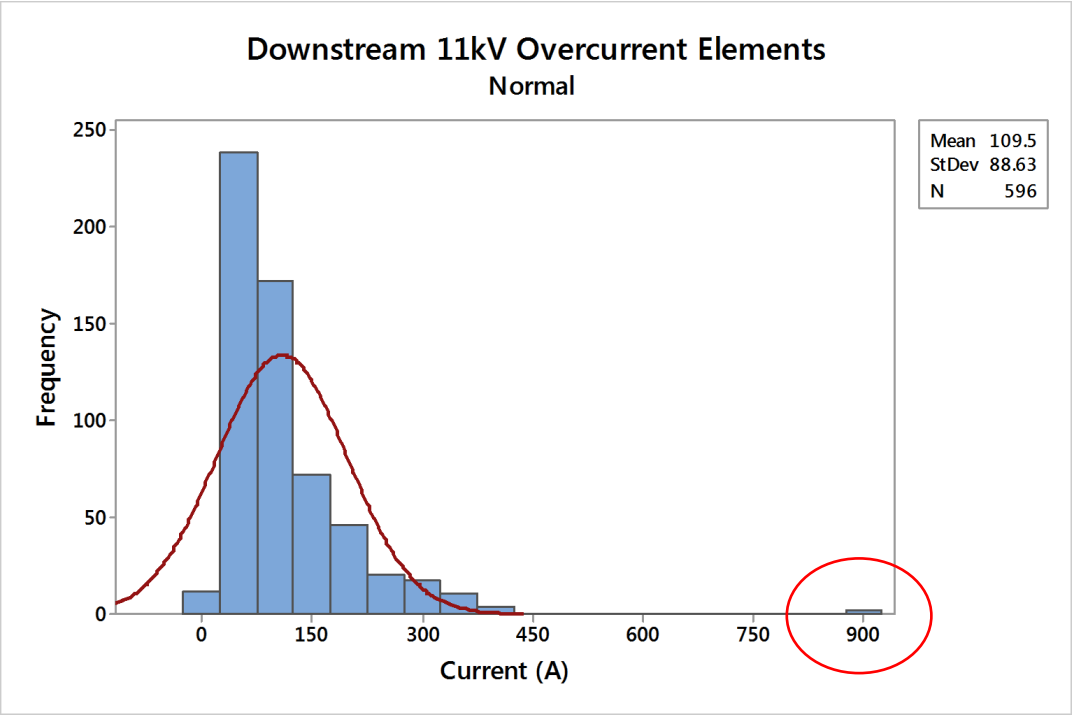


Figure 30: Distribution of downstream 11kV Overcurrent tripping thresholds (SQL Query 2)

4.3.3.2. Benchmarking of Phase Multiplier

The result of the SQL query for downstream phase multipliers is shown in Figure 31. The calculated mean and values within one standard deviation are indicative of the typical setting required to be applied to protection IEDs. A proposed setting within this range would be deemed appropriate suggesting the method can provide validation for a proposed setting and will also identify those settings that outside typical ranges as indicated by the red circle in Figure 31.

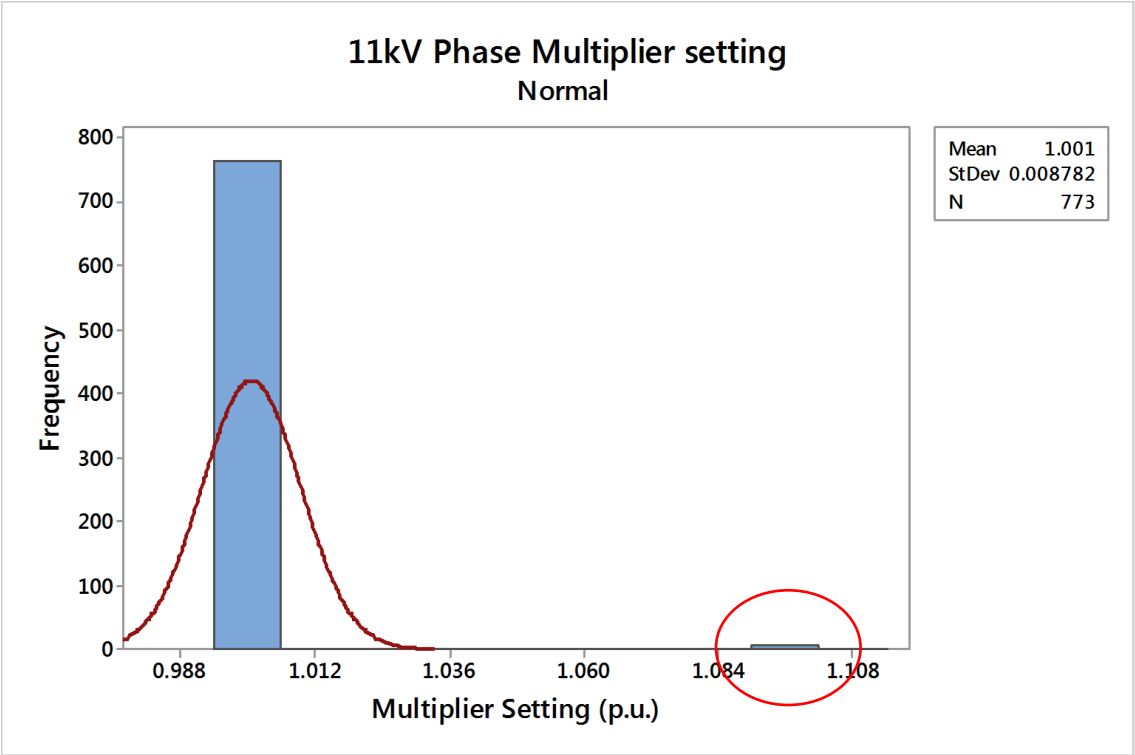


Figure 31: Distribution of Phase multiplier thresholds (SQL Query 2)

4.3.3.3. Benchmarking Earth Fault Thresholds

The result of the SQL query 1 for the feeder bay Earth fault is shown in Figure 32. It is evident by the graph that the tripping thresholds range is diverse in both its magnitude and frequency. The mean value and standard deviation returned values that align with Ergon Energy's protection philosophy. Whereby protection reaches for earth faults is calculated using an additional fault impedance of 50Ω. For an 11kV system with a 50Ω fault the highest fault current used for reach calculations is 127A. Using the standard reach factor of 2 the maximum setting is expected to be 63.5A.

The outgoing feeder results provided a mean of 47.52A and one standard deviation from the mean of 16.03A. One standard deviation above the mean is 63.5A and one below is 31A. This query was successful in providing an effective tool to determine a valid setting for the earth fault thresholds applied to outgoing 11kV feeder bays. If the proposed setting is within one standard deviation of the mean it is expected to maintain appropriate reach.

Comparison of the proposed setting to that of values within one standard deviation of the mean would provide confidence that the setting is within typical magnitudes. As mentioned previously this method also is able to identify a non-typical setting. An example of this is the red circled setting in Figure 32.

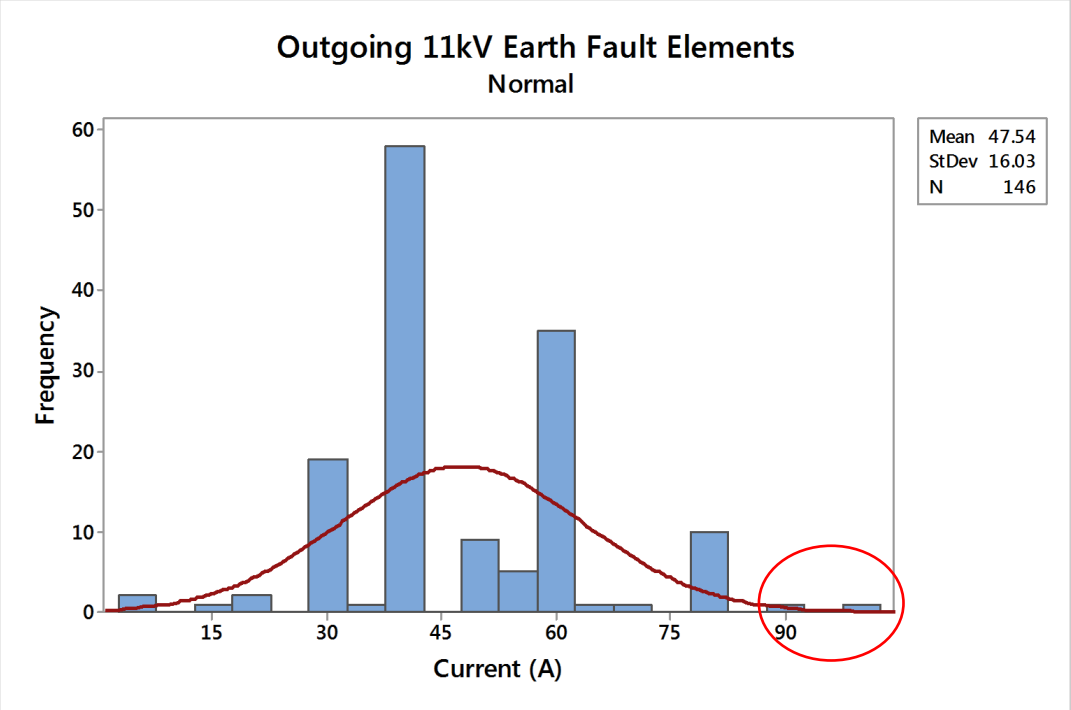


Figure 32: Distribution of Outgoing 11kV Earth Fault tripping thresholds (SQL Query 1)

The result obtained from SQL query 2 for downstream Earth Fault thresholds are shown in Figure 33. The results of this query provide a mean of 26A and one standard deviation from the mean of 11A. This calculates to a magnitude of 37A for one standard deviation above the mean. The maximum expected threshold applied to the upstream protection IED at the substation would be 63.5A. To provide current grading between the upstream and downstream devices, the downstream earth fault threshold would be set to 80% of upstream earth fault threshold. This equates to approximately 50A. The value of 50A is below the preferred 63.5A, therefore would be deemed as an appropriate setting. The result of the SQL query would deem this value not appropriate as it falls outside one standard deviation of the calculated mean. This indicates that this query would not be an appropriate validation tool for all earth fault settings applied to downstream Protection IEDs.

The query did demonstrate the method can be used as an indicator identifying those settings that are outside what is typically applied as shown by the red circle in Figure 33.

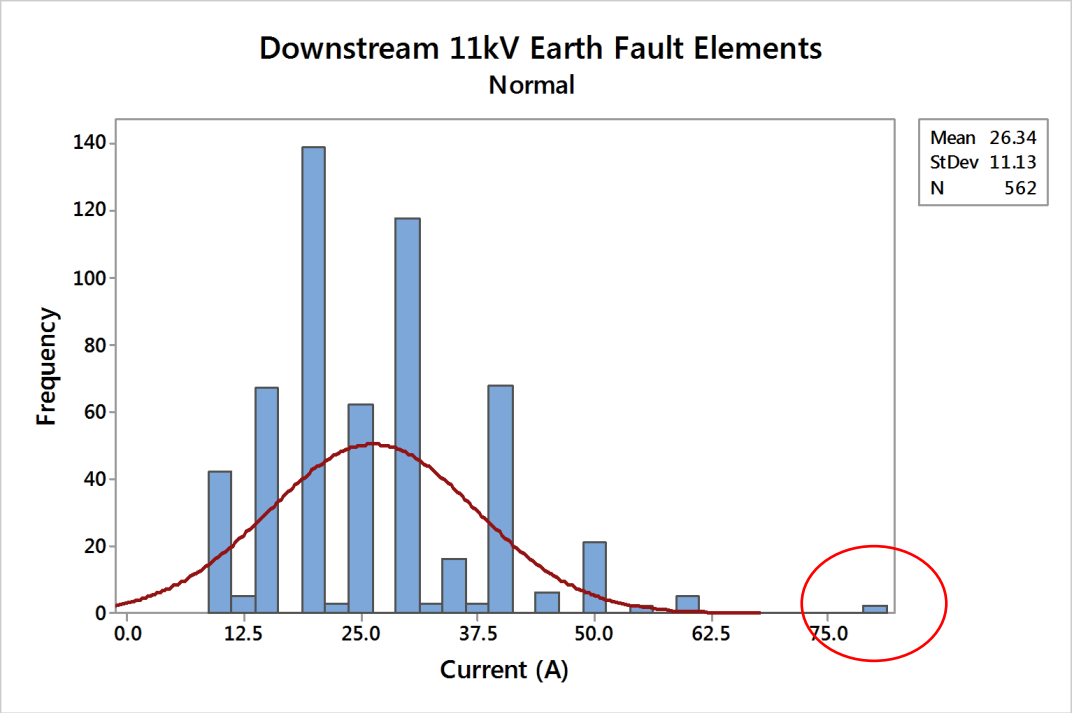


Figure 33: Distribution of downstream 11kV Earth Fault tripping thresholds (SQL Query 2)

4.3.3.4. Benchmarking Sensitive Earth Fault Thresholds

The result of the SQL query 1 for the outgoing Sensitive Earth Fault is shown in Figure 34. The calculated mean and one standard deviation is indicative to the typical setting applied to an outgoing 11kV feeder and a proposed setting within this range would be deemed appropriate. Therefore the results of this query can be used to verify the setting applied for SEF applications at bay level as discussed in section 4.3.2.5 and identify any non-typical setting.

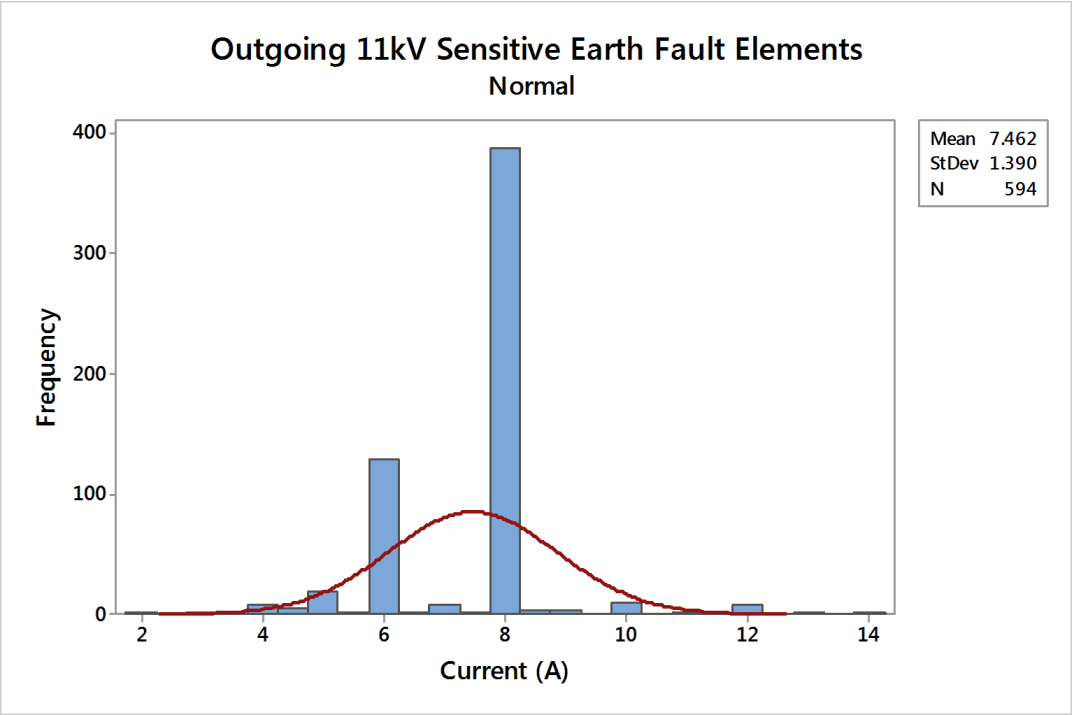


Figure 34: Distribution of Outgoing 11kV SEF tripping thresholds (SQL Query 1)

The result of the SQL query 2 for the outgoing Sensitive Earth Fault is shown in Figure 34. The calculated mean and one standard deviation are indicative to the typical setting applied to downstream protection IEDs and a proposed setting within this range would be deemed appropriate on the condition it maintain coordination with the upstream device. Therefore the method can provide an indication that the proposed setting is within typical magnitudes and will identify those settings that outside what is typically applied.

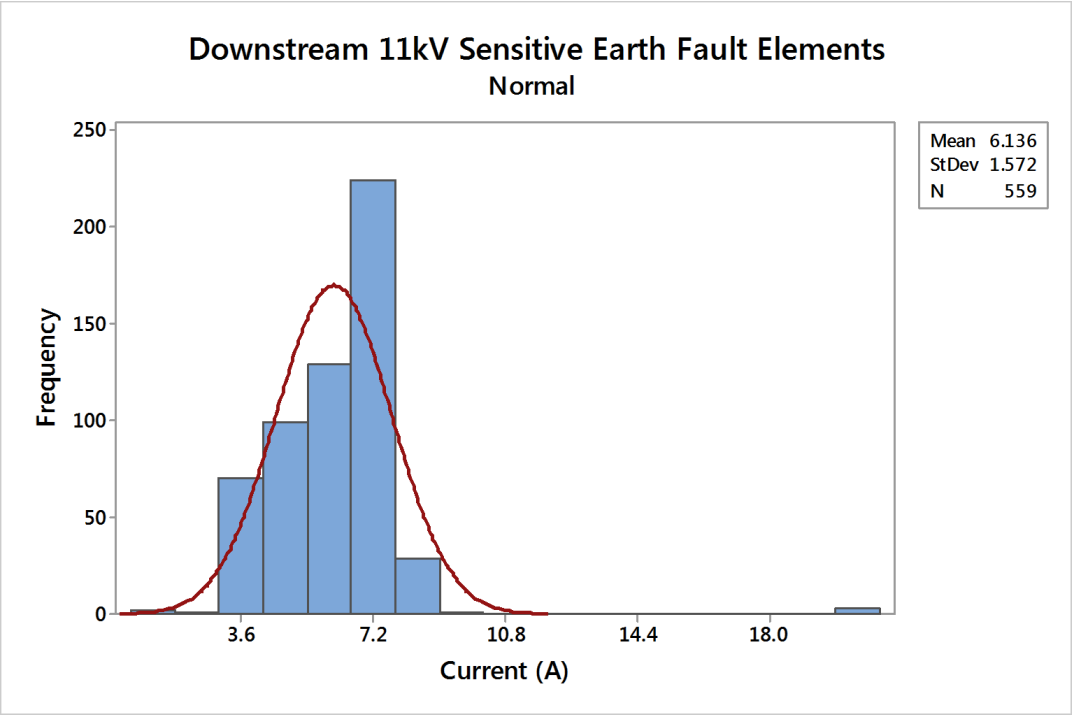


Figure 35: Distribution of downstream 11kV SEF tripping thresholds (SQL Query 2)

4.3.3.5. Benchmarking Outcome

The aim of this benchmarking was to try and establish the mean and standard deviation for critical settings that may be used to critique a proposed setting in the protection setting report. Owing to the topology and the design of distribution feeders the result of the analysis for some of the critical settings returned more of an indication than a defined value which could be benchmarked against.

The reason for this is by design a distribution feeder's conductor sizes and lengths change across its entire route in support of network and supply requirements. These varying attributes impact on the overall impedance of the line which also varies the positive, negative and zero sequence components. The fault levels calculated are reliant on the result of these system impedances and in turn these levels dictate the protection reach requirements and the tripping thresholds applied to the protection IED. Owing to this outcome it was consider that there would no advantage to further data mine to perform a more granular analysis as described in section 3.3.2.1.

4.3.4. Magnitude of change

Another method examined was to measure the magnitude of change of a proposed for an existing installation setting. As described in section 4.3.2 critical criteria for determining a setting is the Protection Reach Factor. These reach factors could be used in conjunction with the existing setting to validate the proposed setting by analysing the magnitude of change. Where the proposed setting value is less than the existing setting then a comparison is not required as this would increase the Protection Reach Factor providing additional sensitivity for network faults. Where the proposed setting is increased a mandatory comparison is undertaken on the premise that protection reach may be compromised.

An example was undertaken by using the data already collected for the downstream earth fault tripping thresholds (SQL Query 2) which provided listings of existing setting and proposed settings. Where a difference between both setting was identified these were captured and imported into an excel spread sheet. Conditional formatting was applied to the list of proposed setting to verify whether the increase in magnitude was within limits. The conditioning applied assumed the existing setting complied with the minimum Protection Reach Factor of 2 (as described in Table 5) for system normal. The maximum increase deemed appropriate for an Earth Fault setting would be an increase which maintained a Protection Reach Factor of 1.3 for backup applications; a setting above this magnitude would require further verification. On this premise the list of installed settings were then compared against the following calculation:

$$\text{Proposed Setting} > \frac{\left(2 \times I_{ps}\right)}{1.3} \tag{1.4}$$

Where:

- Ips – Existing Setting

Where this condition calculated as true the installed setting was flagged in red prompting further verification.

Table 6 provides the results of this calculation applied to the downstream 11kV Earth Fault elements captured by SQL Query 2.

Table 6: Results for magnitude increases using conditional formatting

Proposed Setting	Existing Setting
22	45
30	50
40	50
40	20
25	30
15	20
15	10
20	30
10	15
30	25
20	30
20	15
20	13
45	20
15	10
20	30
40	15
40	15
30	20

4.3.5. Frequency of change

Frequency of change was considered to identify either an inexperience setter was delivering settings that were not appropriate for the application or where there may be an inherent issue with the application or installation the protection IED was designed to protect. The Ergon Energy's Protection Database System (PDS) was again mined to try and identify multiple changes in short succession. The method of the data mine was to first identify multiple changes of a single protection IED with an open time internal. This found no excessive setting changes to a single device, although an analysis of this type proved difficult as to the determination of what is considered as excessive changes. However mechanisms to capture each setting change for a single device as a count could provide the data to establish a bench mark of an excessive setting.

4.4. Development of an improved Configuration delivery process

Where a discrepancy is identified within the Protection Setting Report, configuration file and Protection Setting Request (PSR) confusion lies around which component is the correct source of information. The Protection Setting Report is the primary document of the workflow and all settings applied to the configuration files and Protection Setting Request (PSR) are to be derived from this document. Improvements to the workflow employed a top down approach in order of the Protection Setting Report, configuration file and Protection Setting Request (PSR).

The examination of existing workflow identified only one check point which required all three components being checked at the same time. As shown in the initial fault tree analysis peer review checks are recent additions. The reviews however are not descriptive in the requirements of the checks that should be undertaken to maintain a consistent output. It was identified more descriptive steps should be applied to the workflow with reference to the generic process (CIGRE Working Group B5.31 2013) discussed in section 2.4. Three quality checks are recommended to improve the existing Protection Setting Workflow.

- Quality Check 1
- Quality Check 2
- Quality Check 3

The locations of these checks within the existing workflow are shown in Figure 36 and the quality checks required are detailed in the following sections.

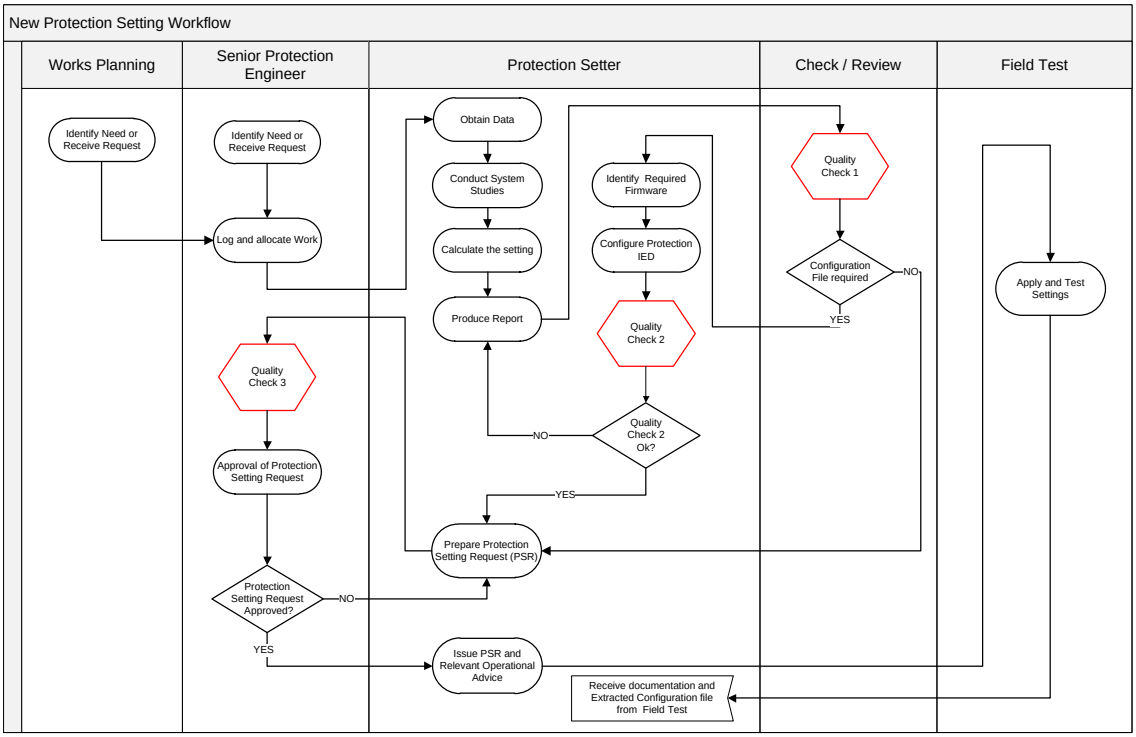


Figure 36: New Protection Setting Workflow

4.4.1. Quality Check 1

The existing Protection Setting Report template employed concentrates on the calculations and documenting the system configuration that determine the value of thresholds and characteristics that are to be implemented. Methods to verify these values have been discussed in Section 4.2. Where the application is considered a standard installation all functional, control and indication logic are described in standard configuration documentation for the prescribed application. The description of this logic will not appear in the Protection Setting Report. In the existing workflow the report is created in isolation to the configuration file providing opportunity for these discrepancies, while not errors, benefiting from being minimised.

As part of Quality Check 1 the following key items are recommended to be checked with additional attention of those items identified in Appendix C.2 and C.3, but are not limited to;

- Tripping and Time Thresholds
    - Required Protection Reach Factors are met
    - The intended protection element to be used is correctly documented
- Time Characteristics

    - Appropriate time grading is maintained
    - The intended timer is correctly documented
    - The intended time characteristic is correctly documented
- Control, indication and Functional Logic
    - Review of any non-standard application requirements

The last point is also a consistent discrepancy defined by the progressive survey; and as shown in the fault tree analysis in Figure 16 introduction of non-standard control, indication and functional logic functions have the potential to increase the overall error rate due to the setter or even checker being familiar with adding such features. Ergon Energy have implemented standard configuration files which have been tested and commissioned and have history of correctness. Implementation of non-standard features relies on setter, checker and eventually the field test staff to verify whether they provide the intended result. The Protection Setting Report should document the required deviations from the standard and the reason that has prompted the implementation of non-standard features. Furthermore these non-standard features applied to the Protection IED software should be tested and verified to ensure the configuration file is operating as design (Standards Australia 2011). This mechanism is considered to reduce the probability of error for these non-standard features from a "Complicated Non-Routine task" to a "Routine task with care" within the fault tree analysis in Figure 16.

Section 5.2 describes a new verification method which can provide such verifications in a controlled and well documented environment; the latter is particularly import to provide the opportunity to continuously improve the workflow.

4.4.2. Quality Check 2

At this stage of the workflow the protection setter should have identified the firmware of the intended Protection IED prior to developing the configuration file.

One of the predominate responses obtained from the surveys was that requested thresholds and time characteristics were not valid settings i.e. there was a discrepancy between the final calculated settings as documented in the Protection Setting Report and

what could be applied the protection IED. This is owing to the Protection IED elements' setting resolutions; meaning the Protection IED will not accept the exact calculated value the setter may wish to employ. In this case the protection setter is required to make a judgement on the accepted setting in comparison to the calculate setting. If the Protection IED value is deemed acceptable and this change is not reflected within the Protection Setting Report a discrepancy now exists.

To reduce these occurrences Quality Check 2 has been introduced leveraging of the comparison features of the vendor's software and Ergon Energy's suite of Standard configuration files. This check is performed by the setter after Quality Check 1 is completed and with recommended actions described in Figure 37.

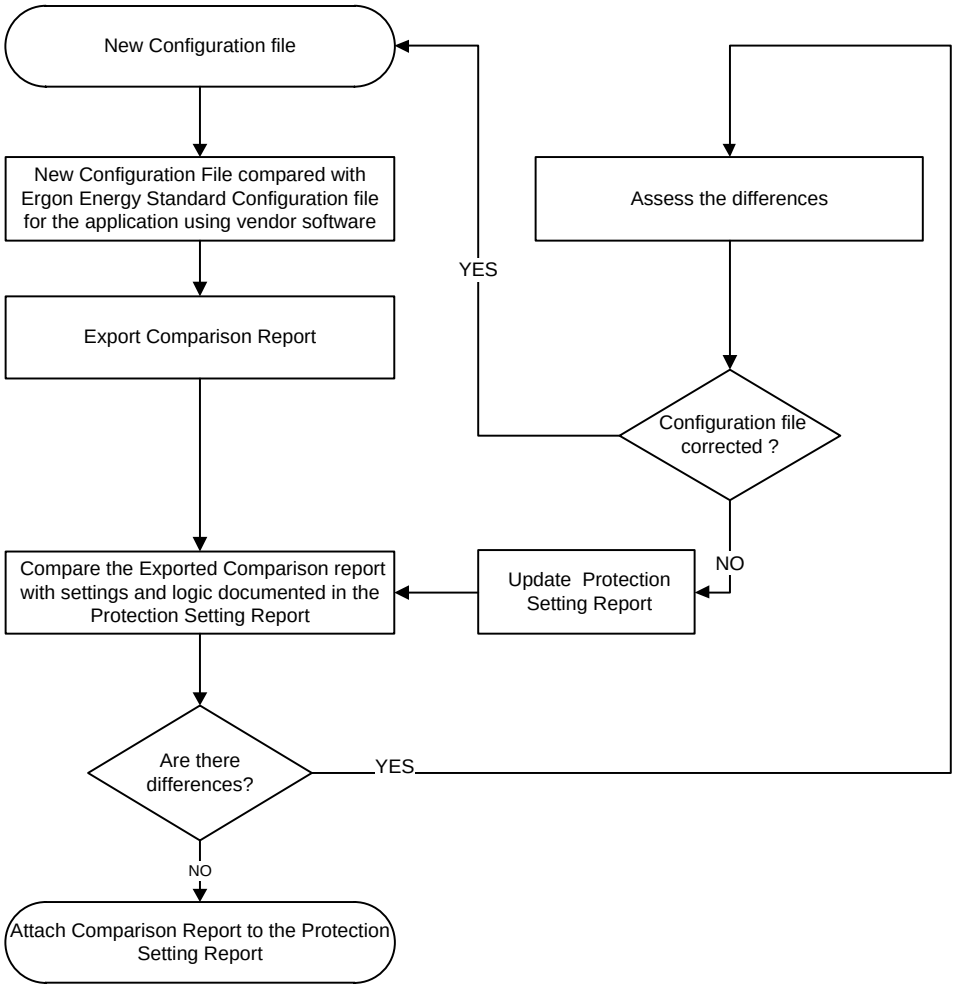


Figure 37: Recommended action for Quality Check 2

4.4.3. Quality Check 3

At this stage the Senior Protection Engineer is required to approve the Protection Setting Request (PSR) considering the information provided by the Protection Setting Report and configuration file. The required checks at this stage are:

- The PSR is verified against the comparison report of the configuration ensuring all applied elements and settings of the Protection IED are present.
- Any change in control, indication and functional logic is checked for;
    - Correctly documented in the Protection Setting Report in comparison to the configuration file
    - A specification has been developed to enable testing of the non-standard features applied to the Protection IED.
- The correct firmware is identified and documented

4.4.4. New Protection Setting workflow analysed

The new Protection Setting workflow was then analysed using the same techniques outlined in section 4.1.

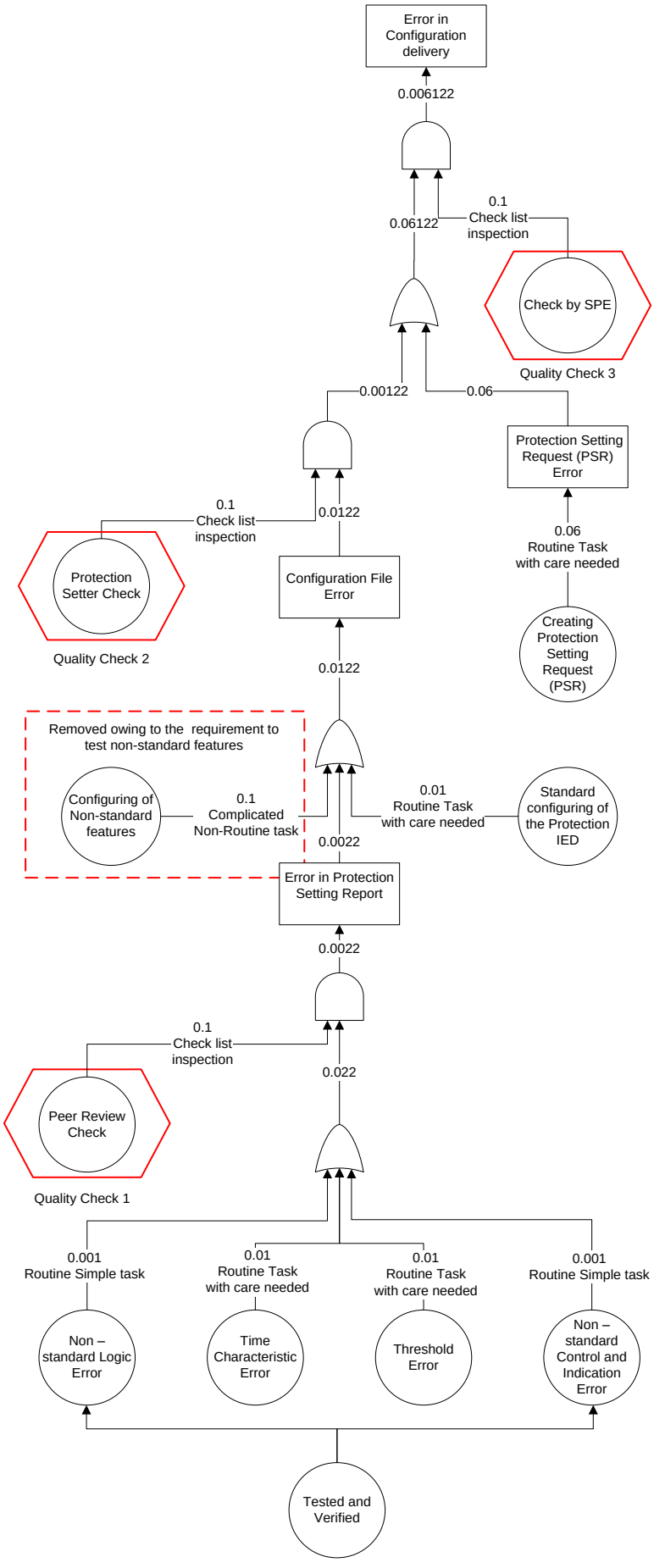


Figure 38: Fault Tree analysis for new Non-Standard configuration delivery

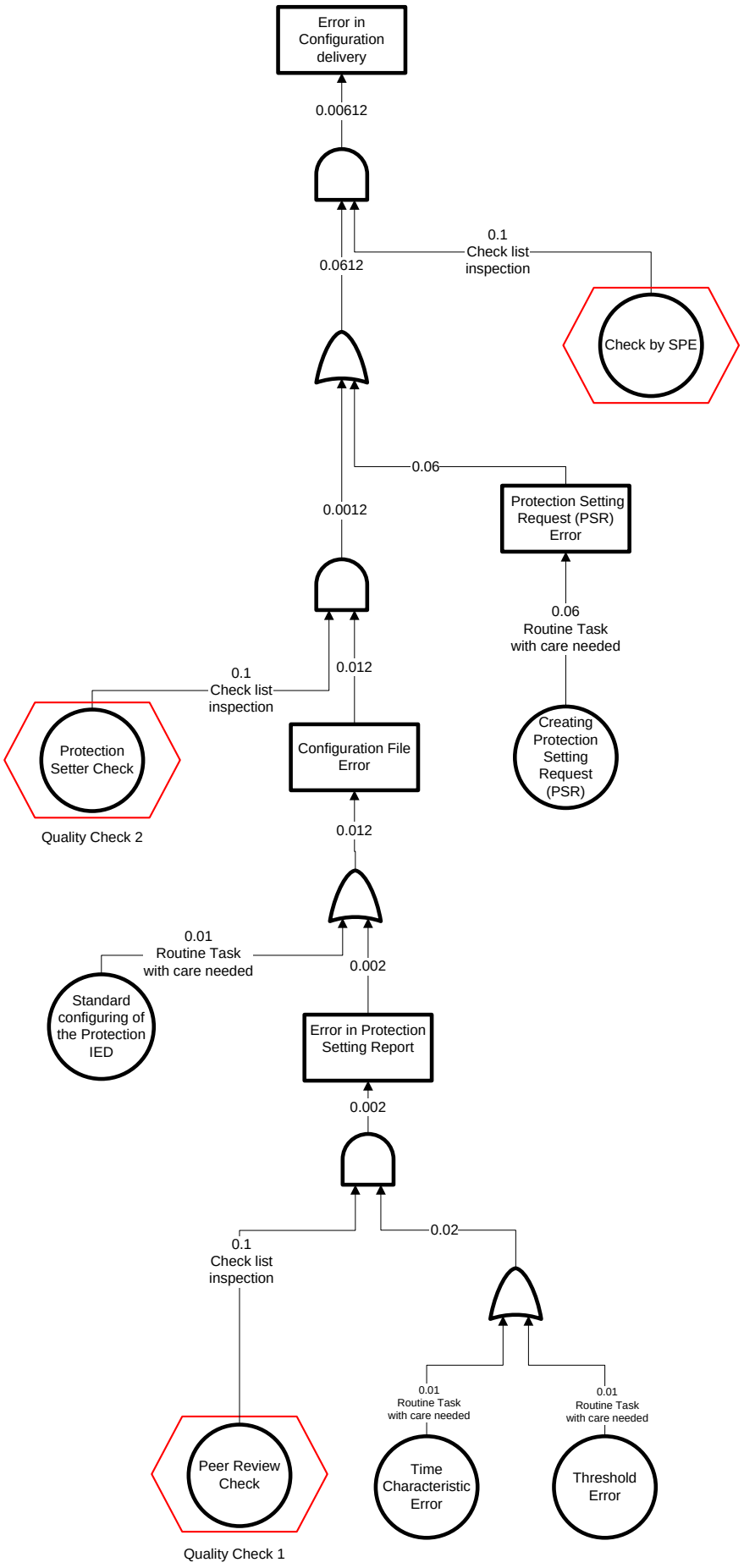


Figure 39: Fault tree analysis of the new Standard configuration delivery

4.4.5. Results of Fault Tree Analysis

Figure 38 and Figure 39 show the change in the probability of errors for both the non-standard and standard. The injection of the prescribed quality checks in Section 4.4 provides a configuration delivery error probability of approximately 0.6%. When compared to the analysis of the existing workflow with a probability error in the range of 22.36 % to 33.36%; the recommendations provide the opportunity to significantly improve configuration development using the new workflow.

4.5. Chapter Summary

The chapter examined the effectiveness of the existing workflow and by doing so identified the root causes of configuration delivery. A new work flow was developed and its improvements were also analysed with a favourable outcome. Methods to verify and validate protection settings applied to the Basic IED types were analysed to determine their effectiveness to be used as validation techniques for power system settings.

Those methods that were found effective could be employed using the existing Protection Database System (PDS) or introduced as part of reporting capabilities within a Configuration Management System (CMS). The reporting could be structured around those methods discussed reducing the need for a continual check, allowing more concentration on those system settings that are unique due to the design of the distribution network. It is recommended the use of such tools should be regularly audited to ensure they have not been compromised and are still effective in manner in which they were intended (CIGRE Working Group B5-09 2006).

Chapter 5

Remote Delivery of Protection IED Configurations

This chapter discusses the assessment of a remote configuration process against the regulatory and legislative requirements imposed on Distribution Network Service Providers (DNSPs) with respect to testing of protection IEDs; combined with the examination and assessment against traditional processes used to verify Protection IED configuration files to be installed into the Basic IED type devices.

5.1. Traditional Configuration Management and Delivery

Historically a configuration was considered fit for purpose once it had been written to the device intended for service and validated using secondary injection to apply sinusoidal voltages and currents. This approach typically identified issues such as:

i. Consistency issues between PSR, setting file and Protection Setting Report
ii. Unintended feature interaction introduced by implemented functional logic
iii. Unexpected operation of the Protection IED for application settings
iv. Failure of the Protection IED to operate (testing of device hardware i.e. A/D converters and IED I/O)

Items (i) to (iii) directly relate to the Protection IED's software which encompasses the aspects of configuration application. These tasks are currently undertaken across multiple workgroups within Ergon Energy and in some cases across extended time periods.

Item (iv) relates to the Protection IED hardware which in essence is the devices ability to operate when called upon. Item (iv) could be considered to be independent of the configuration management approach as a robust configuration delivery process would not be expected to create physical inoperability of a Protection IED. Item (iv) is managed by maintenance and monitoring processes (Zimmerman 2014).

5.1.1. Traditional Delivery Process for Protection IED Configurations

The existing configuration management system typically has the protection and field test staff working together to implement Protection IED configurations. The traditional delivery process of a protection IED configuration file is shown in Figure 40. A detailed description of each component of the process is discussed in the following sections.

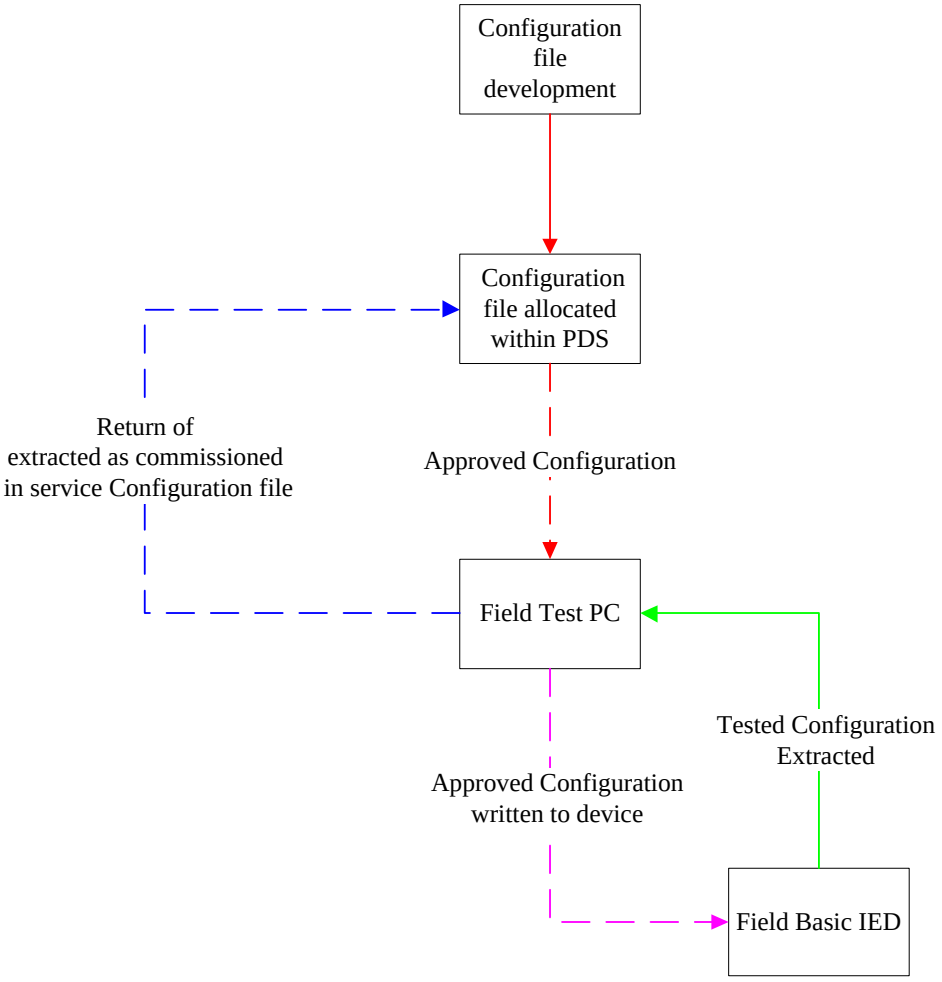


Figure 40: Traditional delivery process for Protection IED configurations

5.1.1.1. Configuration file development

The responsibility of the protection setter is to develop configuration files by selecting the appropriate file template and applying the required modifications based on the application. Improvements to this aspect of configuration management have been investigated and addressed in section 4.3.

5.1.1.2. Configuration file allocated within PDS

The configured file is identified as per standard naming conventions and stored in Ergon Energy's Protection Database systems (PDS) for engineering approval. Once approved, the configuration file is issued for installation.

5.1.1.3. Field Test PC

A field Test person extracts the approved file from the Protection Database System (PDS) to a test PC. The field Protection IED's make, model and installed firmware is confirmed against the issued documentation and configuration file to ensure compatibility prior to uploading the configuration file.

5.1.1.4. Field Protection IED under Test

The field Protection IED's make, model and installed firmware is confirmed against the issued documentation and configuration file to ensure compatibility prior to uploading the configuration file.

5.1.1.5. On-Site Configuration file delivery

The issued configuration file is downloaded to the Protection IED using vendor software. Injection testing of the configuration is undertaken. On completion of the testing the configuration file is extracted from the Protection IED to the Test PC. A comparison between the issued and extracted file is performed and where discrepancies and found they are reported to the protection setter. Where a file comparison reports no discrepancies the extracted file is identified as per the standard naming convention and

the configuration file along with the completed Protection Setting Request (PSR) is returned to the protection setter.

5.1.1.6. Returned Documentation and Configuration file

On receipt of the extracted configuration file and completed PSR, the protection setter performs a comparison of the issued and extracted files to confirm no discrepancies exists and if correct, the extracted file is then imported into the Ergon Energy's PDS and recognised as the commissioned / in service file; and is used as the reference file for future reconfigurations.

5.2. Remote Configuration Management and Delivery

5.2.1. Overview

Implementation of a remote configuration delivery process meant an alternate verification method was needed to ensure that best practice is maintained. To sustain similar verification methods the setting development stage was expanded to incorporate laboratory testing of the configuration files emulating the tasks outlined in sections 5.1.1.3, 5.1.1.4 and 5.1.1.5. The proposal is to test the proposed configuration in an identical device to that in the field. Once the new process was developed an evaluation against current practices was undertaken. An overview of the expanded process is shown in Figure 41.

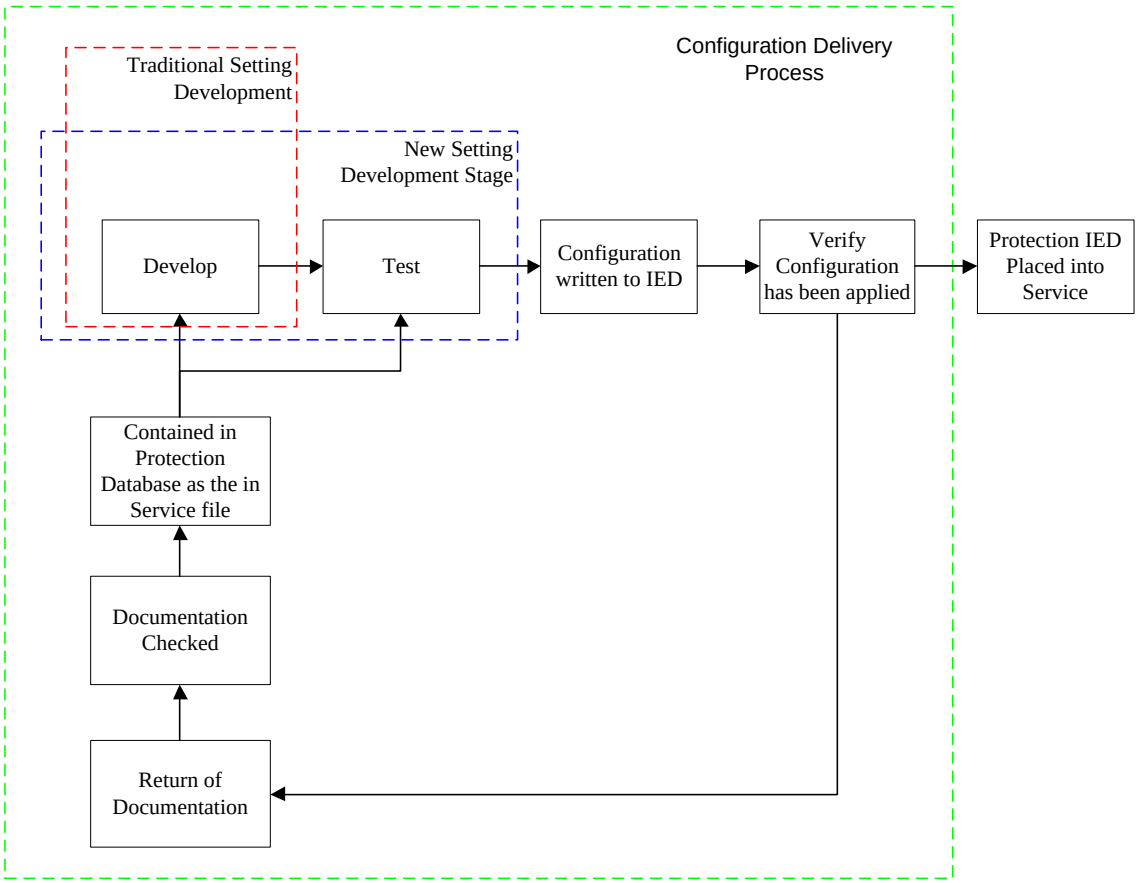


Figure 41: Overview of the change in configuration delivery

5.2.2. Remote Delivery of Protection IED Configurations

During development of the new delivery process an anomaly was found with a Basic Protection IED installed on the Ergon Energy network. The anomaly was found not to impede the Protection IED's ability to operate for network faults but would impact on the ability to verify the installed configuration file via a remote delivery process. The failure mode identified would modify an extracted file, meaning that if the extracted file was download to the Protection IED and retested, it would provide different results compared to the original configuration test (see case study in Appendix E.1). Leveraging off the case study and existing traditional delivery methods an improved process was developed changing the current techniques of how the issued and extracted files are verified and managed.

The traditional delivery emphasis is on the extracted file becoming the master file on completion of the configuration delivery. The case study in Appendix E.1 found the extracted configuration file was not a complete representation of the installed

configuration file. To correct this error a manual change to the setting file would be required, which if performed, suggests the file is no longer the tested in service file. If left uncorrected, the extracted file (master) contains an error. Under the traditional process the master file is kept and used for future reconfigurations of the Protection IED. The design of the new delivery process eliminates the occurrence.

The process for file verification is shown in Figure 42 and is as follows:

ΔS_L is representative of any changes that are introduced as part of the file download process. These errors are identified when the file is tested using traditional means in the LAB test device.

ΔT_L is representative of any changes that are introduced by the extraction of settings from the LAB IED under test.

ΔS_F is representative of any changes that are introduced by downloading the configuration file to the field IED. These changes cannot be explicitly measured.

ΔT_F is representative of any changes that are introduced by the extraction of settings from the field IED. This is not explicitly measureable.

Ideally all of the Δ values will be zero (representing no change) during the upload and download process.

The file in the field IED is deemed to be the same as the intended file provided that $\Delta T_L = \Delta T_F$ and the injection test in the laboratory proves that no ΔS_L has occurred. Any corruption that has occurred on the download or upload to the field IED that was not evident on the device under test, would be indicative of a remote configuration problem. This would mean that the extraction process between the two devices did not match $\Delta T_L \neq \Delta T_F$. The download process between the two devices did not match $\Delta S_L \neq \Delta S_F$. Alternatively both the download and upload process did not match. A case may exist where the download and upload from the field IED created and then corrected an error in a configuration file. This was deemed an improbable scenario as the download and subsequent upload corruption would be of the same master file used in the laboratory and would have to create and then correct an error over a communications system that employed error checking.

An additional check $\Delta T_L = \Delta S_L$ may be performed to ensure vendor performance (e.g. download and upload are the same) however this check is not one that would help identify the remote configuration delivery was successful.

Once a successful verification has been confirmed ($\Delta T_L = \Delta T_F$) ΔS_L is considered the master file. This process is deemed to be more robust compared to that of the traditional delivery method as it maintains a master configuration file that is free of error. An overview of new process is shown in Figure 42 with the following sections describing each step.

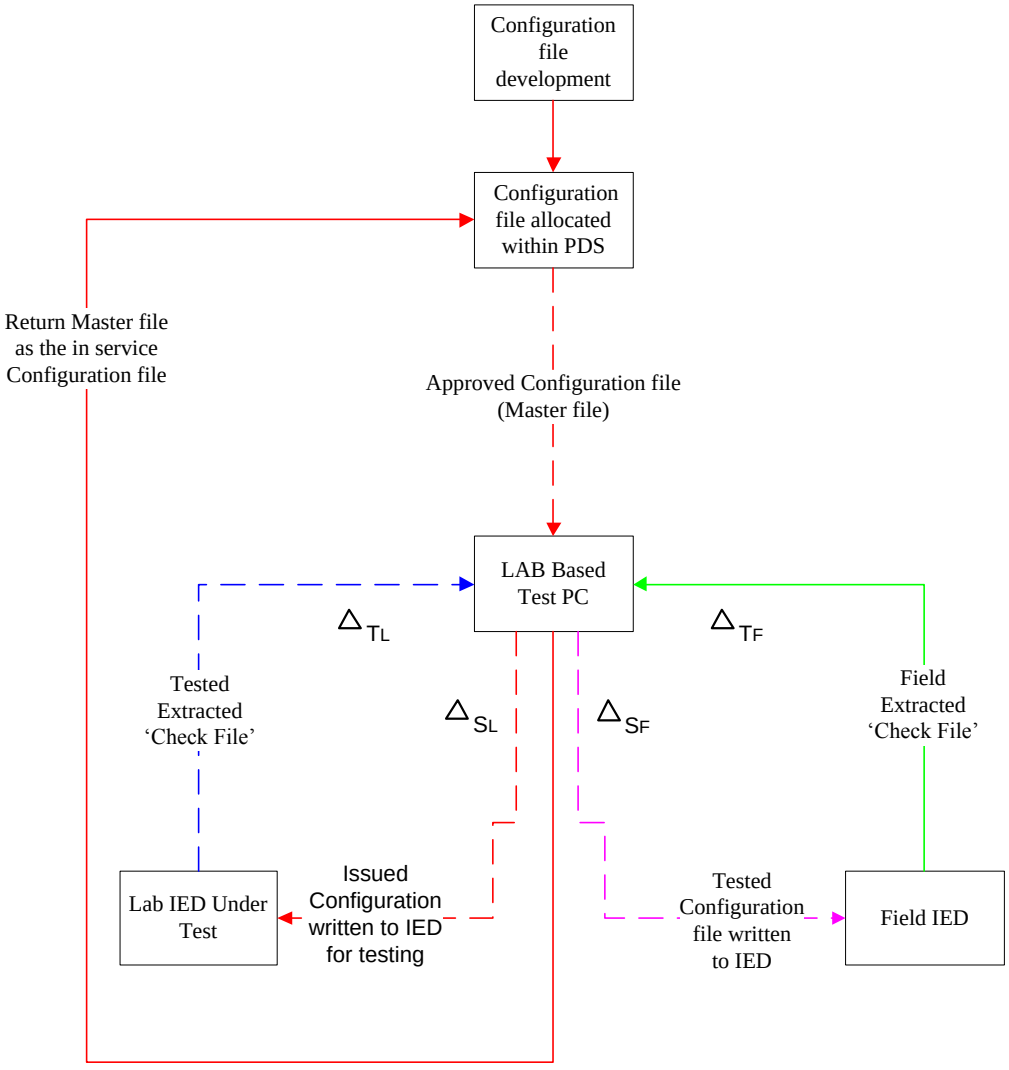


Figure 42: Remote delivery process for Protection IED configurations

5.2.2.1. Configuration file development

There is no change to this step as described in section 5.1.1.1.

5.2.2.2. Configuration file allocated within PDS

The configured file is identified as per the standard naming convention and stored in Ergon Energy's Protection Database System for engineering approval. Once approved, the configuration file is issued so that it may be installed.

5.2.2.3. Test PC

This case the test PC is loaded at a centralised test facility. The test PC is operated by personnel who are knowledgeable in the operation and functionality of protection IEDs under test. It is envisage field test personnel would undertake testing at the centralised facility following all requirements under Standard Work Practice (SWP) SP0518.

The issued configuration file which is written to the laboratory based protection relay under test shall remain the primary (master) configuration file for the duration of the configuration delivery process.

5.2.2.4. Laboratory Protection IED under Test

This stage involves tests to validate the software, settings or both as well as ensuring the software does not perform any unintended functions or operations once installed into the Protection IED (Standards Australia 2011). Verification that Protection IED under test is the same as the intended field Protection IED is essential. The two devices need to be from the same vendor and have consistent model numbers and firmware versions.

In addition to those tests prescribed in Standard Work Practices (SWP) SP0518 an additional check is required. This check shall consist of injection of balanced 3 phase sinusoidal voltages and currents simulating load conditions. This is to confirm that for a configuration delivery that the Protection IED does not respond abnormally on receipt of the configuration file, further confirmation of an expected response during the delivery process.

To ensure that the settings are not modified by the upload process the setting files will only be deployed in one direction for application as shown in Figure 42. The configuration at this stage will be:

- Provided by the setting developer to the setting tester
- Downloaded to the device under test
- Tested to ensure that the configuration performance is as expected

On successful completion of testing the configuration file is now extracted and is allocated as the configuration delivery ‘Check’ file. At this stage the primary (master) configuration file is ready to be written to the remote device.

5.2.2.5. Operational and functional checks

The following operational checks shall be undertaken prior to configuration delivery;

- Record the operational state for protection control functions e.g. SEF enabled, A/R enabled
- 3 phase load measurements shall be recorded and compared against the proposed overcurrent setting. This is to migate the risk of a mal-operation for an inappropriate threshold with respect to load conditions

The following functional checks shall be undertaken prior to configuration delivery;

Functional Software –

Functional software checks are used to confirm that the Protection IED to receive the new configuration file is an exact match as the Lab Protection IED with respect to;

- Manufacturer Make
- Manufacturer Model
- Firmware version

Functional hardware–

Functional hardware checks are used to establish hardware health of the protection IED. These checks should confirm the Protection IED;

- Is not exhitbiting a self-monitoring alarm event e.g. watchdog alarm
- Displays correct analogue values confirmed by examination of one or more of the following;
  - Vendor software and SCADA values
  - An upstream Protection IED

5.2.2.6. Configuration Delivery Stage

The tester, using the same laboratory based test PC, remotely connects to the field Protection IED and downloads the master configuration file. When the vendor software reports that the primary file has been delivered an extraction of the configuration file contained within the field protection IED is performed and is allocated as the 'Field IED Check' file. At this stage of the process there are two Check files available; one obtained on completion of testing the laboratory Protection IED as described in section 5.2.2.3 and the other from the field Protection IED. These files are now compared with each other to identify any discrepancies.

A successful comparison of the two extracted check files suggests both the laboratory Protection IED under test and the remote protection IED have responded in a similar manner for the same operation.

The primary (master) configuration file and the field Protection IED Check file are now compared to identify discrepancies prior to returning the primary file to Ergon Energy's PDS as the in service configuration file. Where discrepancies are identified they are to be evaluated and documented. Both check files are now discarded.

5.3. Comparison against Traditional processes

To assess the success of the remote process a comparison between it and the traditional delivery processes was undertaken with reference to Ergon Energy's SWP SP0518; the requirements of each component which the remote process was assessed against has been reproduced at the start of each subsection. A comparison of the strengths and weaknesses of each process is listed in Table 18 in Appendix F.

5.3.1. Overview

Section 6.4 of SWP SP0518 describes the basic testing philosophies that should be employed in relation to setting changes to a protection relay. It is acknowledge that the existing testing methods have historically been employed to provide the appropriate verification of both the setting applied and relay operation. The purpose of this section is to examine and benchmark the remote process outlined in section 5.2 to the applicable requirements of testing described in SWP SP0518; with an overview of these requirements shown in Figure 43.

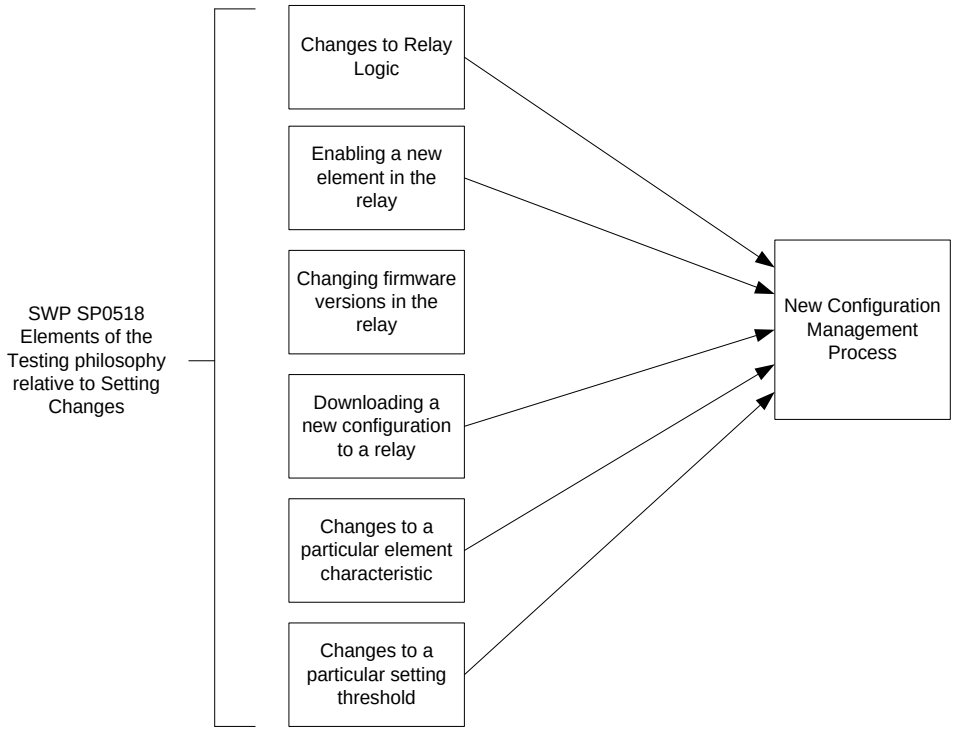


Figure 43: Related SWP SP0518 testing philosophies

5.3.1.1. Changes to Relay Logic

SWP SP0518 states:

> *"There is a requirement to fully retest a protection relay when a functional logic change is made."*

The remote delivery process has bounded the protection relay type to the Basic Protection IED which is typically subjected to configurable pickup and time characteristics. However recent introduction of functional logic has been extended to these devices.

The laboratory testing is able to confirm that applied functional logic is operating as expected and the application of the logic has not introduce any feature interaction with any other enabled function of the Protection IED. The technique of testing a laboratory protection IED of the same make, model and firmware version of the field protection IED ensures the software is operating as intended; and if proven correct, it is expected the hardware of the field protection IED will respond in the same manner as the LAB Protection IED.

5.3.1.2. Enabling a new element in the relay

SWP SP0518 states:

> *"There is a requirement to fully retest a protection relay when enabling a new element."*

This is in response in determining whether the implementation of the new element has introduced an unexpected operation or unwanted interaction with other protection elements and associated features. The remote delivery process is committed to fully retesting the changed configuration within a laboratory environment proving the newly enabled element has no impact on the existing configuration file.

5.3.1.3. Downloading a new configuration to a relay

SWP SP0518 states:

> *"When downloading a new configuration file to relay, all functions must be re-tested. An exception to this is when no new functions are being added (for example a pickup change only) and the relay software has a "compare" function to verify that no file corruption on download has occurred."*

The remote process provides the capability to retest the configuration file in its entirety using a test Protection IED of the same make, model and firmware version as the intended field protection IED; with all tests performed complying with all the SWP SP0518; including verification and comparison of the configuration file delivered to the remote Field Protection IED. The design of the remote process provides the additional benefit in identifying abnormalities as described in Appendix E.1.

5.3.1.4. Changes to a particular element characteristic

SWP SP0518 states:

> *"this requires retesting of the modified element only. Coupled with this will be a "compare" to verify the change has been successfully applied to the relay and no file corruption has occurred"*

The remote process uses test methods outlined in SWP SP058 and again a full retest of the installed configuration file is undertaken fulfilling this requirement.

5.3.1.5. Changes to a particular setting threshold

SWP SP0518 states:

> *"in a digital relay, this does not require retesting of the modified element. However a "compare" is required to verify the change has been successfully applied to the relay and no file corruption has occurred."*

By design a single setting change via remote access may not always be possible and may require a group of settings to be delivered to the protection IED at the one time. The remote process has been designed to support such deliveries and it is recommended that the same process of verification is performed whether there is a single or multiple changes applied to the configuration file. The remote process encompasses verification and comparison techniques which successfully fulfils this requirement.

5.4. Acknowledgement of Regulatory and Legislative Requirements

5.4.1. Electricity Act 1994

A Distribution Network Service Provider (DNSP) must protect its supply network to ensure a safe connection and supply to its customers and also comply with any directives outlined in the National Electricity Rules (Electricity Act, Queensland, 1994 n.d.)

Clause Division 5 (a)(i) of the Electricity Act 1994 states a distribution entity must comply with the National Electricity (Queensland) Law and the National Electricity Rules (NER) and; Provide a safe, maintained and protected supply to its customers and reinforces compliance with the NER.

5.4.1.1. Assessment against the Electricity Act 1994

The laboratory testing discussed in section 5.2.2 prior to the delivery ensures the configuration file for the protection IED is operating as designed and is in accordance with Ergon Energy protection philosophy collectively ensuring that once the configuration installed the protection IED is capable of detecting power system faults maintaining a safe network.

During a remote delivery of configuration files there is a possibility to impact on network reliability owing to how protection IED responds to network disturbances during the configuration delivery. The exposure is dependent on how a Protection IED may respond to the following events;

- Loss of communication between the remote terminal and the protetion IED during remote configuration delivery
- Response to faults which occur during configuration delivery
- Response to configuration delivery during normal supply load

Chapter 6 of the dissertation examines such events. The verification and delivery described in Chapter 5 ensures the delivery process does not contravene the Act.

5.4.2. National Electricity Rules (NER)

Distribution Network Service Providers must also maintain a compliance program to ensure that its protection systems operate reliably (National Electricity Rules).

5.4.2.1. Assessment against the National Electricity Rules (NER)

A compliance program is typically addressed by periodic maintenance which is based on industry experience of Protection IED / relay failure rates.

A Protection IED that is maintained under such programs present a low risk of hardware failure. To protect against the event of a hardware failure Ergon Energy's protection philosophy is to implement backup protection reach for distribution reclosers complying with Clause S5.1.9 (c) of the NER. Where backup protection reach is provided to the Protection IED under reconfiguration and in the event of hardware failure during the remote configuration delivery the feeder is not without protection and is to be isolated

for a fault. This capability maintains a safe network and continues to comply with the NER and the Electricity Act 1994.

However by design an operation of an upstream Protection IED isolating more of the network then would normally be required is not desirable from a reliability perspective. It would be advantageous to ensure that backup protection reach exists prior to a download of a configuration.

Confirmation of backup protection reach is not expected to impose any additional workload to the process. This check would be carried out as part of the protection feeder review undertaken to issue the required change in configuration.

5.4.3. Electrical Safety Regulation 2013

Electrical Safety Regulation 2013 Part 11- Safety management systems Section s234, part 3(b) states;

> *"(3) When a prescribed electricity entity's safety management system is first put into effect or is modified, the entity must give the regulator—*
> *(b) a certificate in the approved form from an accredited Auditor that verifies the safety management system has been assessed and validated to ensure the system comprehensively identifies and addresses the hazards and risks associated with the design, construction, and the operation and maintenance of the entity's works"*

In addition, Division 2 – Earthing and Protection, Section s198 – Performance and other requirements for works, part (h) states;

> *"The following requirements apply for the works of an electricity entity—*
> *(h) electrical equipment intended to form part of the works of an electricity entity must undergo commissioning tests and inspection to verify that the electrical equipment is suitable for service and can be operated safely when initially installed or altered".*

5.4.3.1. Assessment against the Electrical Safety Regulation 2013

Section s234 highlights the need to obtain and review Ergon Energy's safety management system to assess the hazards and risks that are documented especially around design, operational and maintenance of the entity's works to ensure the project objectives are compliant with what is currently lodged with the regulator. The remote process does not impact on Ergon Energy's safety management system as the process will be maintained and operated under the same systems currently employed.

The following describes the methods employed to comply with Division 2, Section s198, part (h) of the Electrical Safety Regulation 2013;

The Remote Protection IED Configuration Delivery described in section 5.2.2 applies to a Protection IEDs which are already in service, have been commissioned and found to be suitable for service. Configuration changes are considered as changes to the software which operates and controls the Protection IED. During a setting change the remote protection IED's hardware connection is not altered and it is expected to operate in the same manner as determined at the time of commissioning.

A software change is still required to be tested to ensure the new configuration is fit for purpose and does not introduce unwanted feature interaction. The process developed for remote configuration delivery, will test and commission the configuration file verifying the configuration file operates as designed and as intended (Standards Australia 2011).

5.4.4. DR AS 2067:2014

F6.12 Protection relays and systems

> *"Consistent with the high degree of dependability required, protection relays and systems should be proven to function correctly at commissioning and at regular intervals. These tests should involve the injection and measurement of operating quantities and should totally prove the system by direct or simulated means." (Standards Australia 2014)*

F6.13 Verification of relay settings;

> *"Verification of relay settings by secondary current and voltage injection and measurement is necessary. Reliance for correct operation should not depend on settings established solely by downloading settings or by*

positioning dials and plugs. The injected current or voltage must have sinusoidal wave shape and the measurements must be by calibrated instruments." (Standards Australia 2014)

5.4.4.1. Assessment against DR AS 2067:2014

In response to DR AS 2067:2014 Draft for Public Comment Australian Standard, Appendix F - Power System Protection, Section F6.12 Protection relays and systems:

Ergon Energy processes for commissioning and maintaining protection schemes aligns with the draft clause with all Protection IEDs being tested and commissioned prior to placing them into service. Regular maintenance programs are implemented on those Protection IEDs located in substation environments.

The remote delivery process is intended to replace commissioning programs for Basic IEDs. Commissioning processes remain intact and are still performed on-site using traditional testing methods to confirm the Protection IED's operation. The intent of the remote delivery process is to support remote configuration changes that do not alter the interaction between the Protection IED's software and hardware. The tests performed involve injection of sinusoidal voltages and currents proving that the software component of the Protection IED is operating as intended and is fit for purpose. Therefore it is considered that the remote delivery process discussed in this dissertation would not be non-compliant to draft clause F6.12

In response to DR AS 2067:2014 Draft for Public Comment Australian Standard, Appendix F - Power System Protection, Section F6.13 Protection relays and systems:

This clause prompted careful consideration in progressing with the remote configuration delivery process owing to the suggestion that protection related functions should be tested using traditional methods of injecting sinusoidal voltages and currents. The proposed process tests the new configuration by installing it into a Protection IED of the same make, model and firmware of the proposed field based Protection IED; and applies sinusoidal waveforms to test its operation.

5.5. Chapter Summary

The chapter has identified the Remote Configuration delivery Process shown in Figure 42 improves upon traditional verification methods and do not impose non-compliance with the presribed Legislative and Regulatory requirements; including existing Ergon Energy standard work practices .

Chapter 6

Response to Remote Configuration

This Chapter details the laboratory testing of a selected Basic IED to assess how it responds to remote reconfiguration and considered external influences that may occur during remote delivery.

6.1. Testing of Remote configuration delivery

The elements under test were those deemed most likely to be changed during a reconfiguration process. It was also important to understand whether an element / setting change is completed as a single change or whether change is delivered as part of a group of settings. This will depend on the manufacture's software design which further strengthens the need to understand the setting change process for all Protection IEDs subjected to remote delivery.

6.1.1. Selected Basic IED

The Basic IED selected for testing was the NOJA RC10 Controller which is fitted to NOJA's line of automatic regulators. A flow chart describing the Basic IED's response for a reconfiguration of the active setting group is shown in Figure 44. An active setting group describes a collection of protection thresholds that are 'active' and are used by the Basic IED to detect network faults. Typically Protection IEDs have multiple protection groups but only one group may be active at any one time. The ACR under test has four available setting groups. The Ergon Energy standard applications for the Basic IED

only permit the use of two groups. One group is used for system normal conditions, and the second typically used for contingency arrangements.

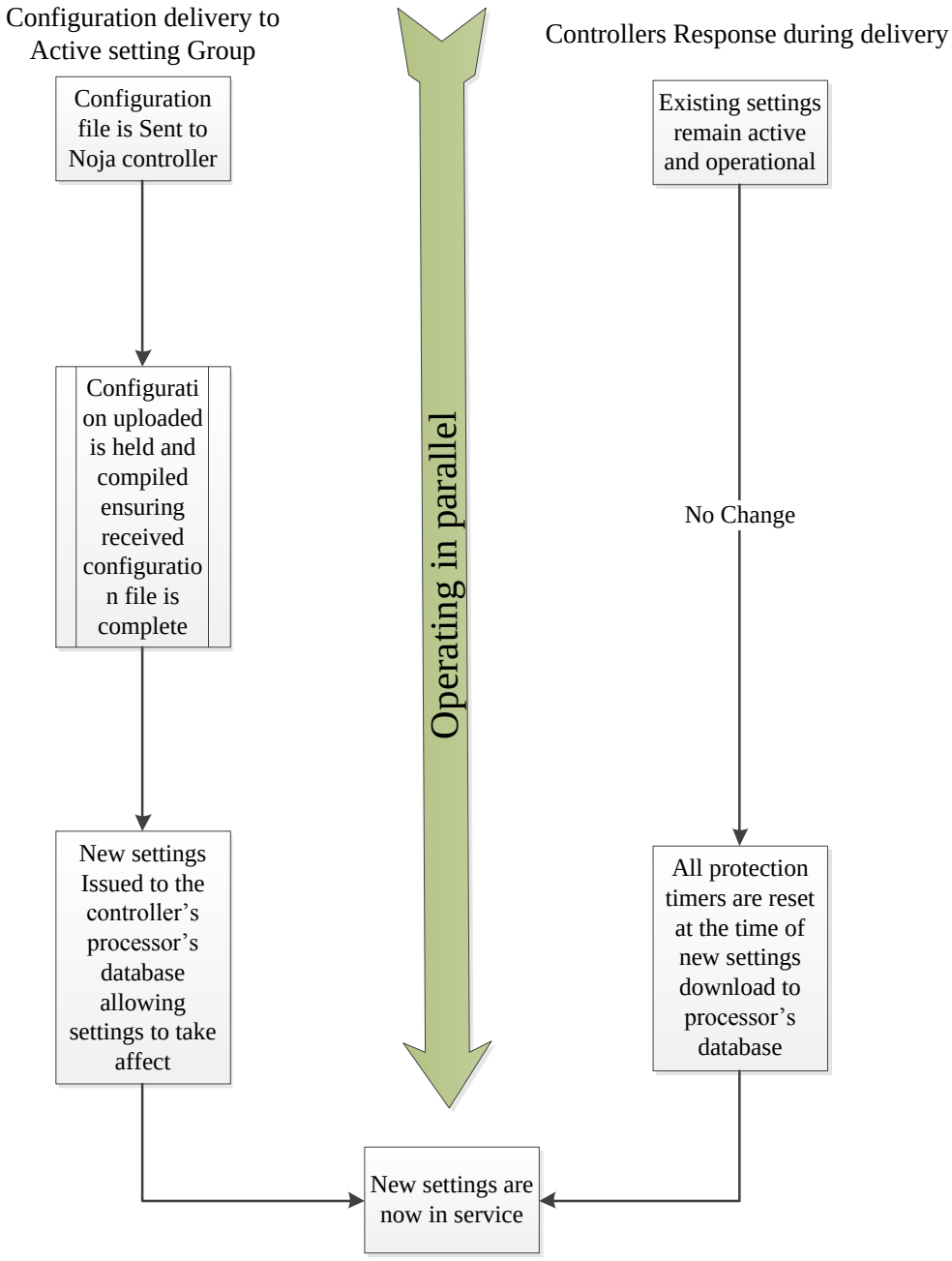


Figure 44: The response of the Protection IED for configuration file upload

6.1.2. Considered Responses of the Protection IED

With the availability of two setting groups it was deemed appropriate to understand how both operated during a configuration delivery operation. After discussions with the manufacturer the tests were designed to explore the responses of both the active and the

inactive setting groups. By design, configuration delivery of a single setting to the tested Protection IED Controller is not possible, meaning a group of settings are required to be delivered at the one time.

The expected responses as described by the manufacturer are;

1) During configuration of an ‘active’ group the response of the controller is to;

- Reset all active timers associated with the active group,
- Apply any reconfigured tripping thresholds,
- Maintain protection throughout the complete configuration delivery.

2) During reconfiguring of an ‘inactive’ group the response of the controller is to;

- Not reset any timers.
- Have no impact on the ‘active’ group settings ensuring that existing protection thresholds and time characteristics remain in service and operational.
- Maintain protection throughout the complete configuration delivey

These responses suggest that no delay of tripping could occur during the delivery of the configuration when delivery is to the inactive group.

6.1.3. Test Environment

The testing was performed using a desktop computer located in Toowoomba and the recloser controller located in Townsville. Sinusoidal voltages and currents were simulated for recloser secondary injection. A series of remote downloading configuration were completed to assess the response of the controller during considered influences. This configuration delivery used the same communication medium currently used by Ergon Energy to provide engineering access to remotely connected Protection IEDs; with the intent to simulate the same process that will be used for future configuration deliveries.

6.1.4. Tests Performed

The tests performed were to confirm the controller’s response as outlined in section 6.1.2 as well as to identifying operational risks. The protection elements tested were

those deemed typical of a required setting change on the 11kV distribution network and included;

- Overcurrent Thresholds and Time characteristics;
- Earth Fault Thresholds and Time characteristics;
- SEF Thresholds and Time characteristics.

6.1.4.1. Considered Operational Influences

The Basic IED was also tested to assess its response to;

- Communication failure of download whilst the device is operating under normal load conditions;
- Communication failure of a download and a network fault after a communication failure;
- A configuration download completed whilst the controller is operating for a network fault.

6.1.5. Controller's Response

Table 7 and Table 8 outline the conditions the configuration delivery was subjected to and the controller's response for the active and inactive group respectively. Simulated network faults applied were Overcurrent, Earth Fault and Sensitive Earth Fault (SEF).

Table 7: Summary of Protection IED's response for the active group settings

Network State	Test Performed	Device Response
3 Phase balanced load	Configuration remotely delivered - overcurrent thresholds below load	Remained stable, operated as expected
Simulated Network Faults	Delivery of a Configuration file with no changes to any enabled protection functions	All elements retested & remained operational and unaffected

Network State	Test Performed	Device Response
3 Phase balanced load	Loss of communication during configuration delivery	Remained stable
Simulated network faults	Retest after previous loss of communication test to ensure protection remained operational	No effect on the existing settings, operated as expected
Simulated network faults	Loss of communication during configuration delivery	All elements unaffected, operated as expected
Simulated network faults	Configuration taken affect whilst a protection timer is active	Delayed tripping was experienced (expected operation)
Simulated network faults	Configuration taken affect whilst a protection tripping threshold is active	Delayed tripping occurred (expected operation)

Table 8: Summary of Protection IED's response for the inactive group settings

Network State	Test Performed	Protection IED's Response
3 Phase balanced load	Configuration remotely delivered - overcurrent thresholds above load	Controller's 'active' group settings remain stable Controller's 'active' group settings remain stable
Simulated network faults	Delivery of a Configuration file with a change in the 'inactive' group's protection functions	'Active' group Protection is maintained and operates as configured. No effect on the SG1 settings, operated as expected.

6.1.6. Testing Outcomes

The recloser operated as per the flow chart outlined in Figure 44. The testing confirmed it would be unlikely that a mal-operation or a mis-operation would occur during a remote configuration delivery for the Basic IED under test. However the effect of the delay tripping should be considered during the risk evaluation for this Basic IED. When a change in configuration is made, the testing highlighted that a change in one element effects all other elements associated with the group.

For example if a overcurrent element is reconfigured and downloaded to the protection IED during a network earth fault the earth fault timer will reset if the configuration takes effect before the timer can expire.

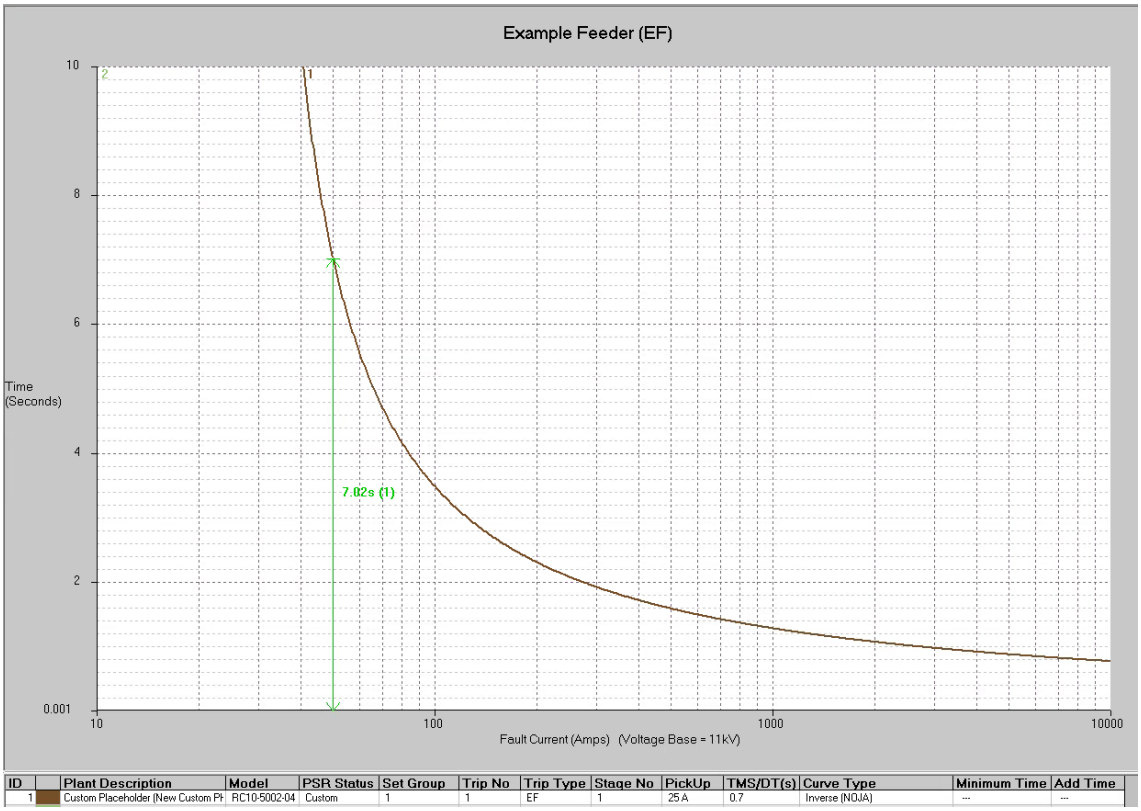
If the earth fault is still detected the timer starts again which delays the protection trip. The extent of the additional time was found to be dependent on when the configuration file takes effect within the Protection IED.

6.1.6.1. Example of delayed Tripping

The IED under test was configured with the existing setting listed in Table 9. A simulated earth fault was injected into the controller to confirm the expected operating times. The inverse IDMT earth fault characteristic is shown in Figure 45 with an expected time of 7.02 seconds for 50A injection.

Table 9 : Protection IED settings

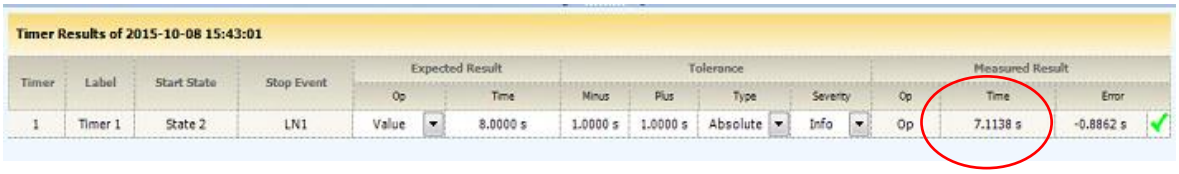
Protection Element	**Existing Setting**			**Required setting**		
	Tripping Threshold	TMS/ Delay	Timing Characteristic	Tripping Threshold	TMS / Delay	Time Characteristic
Overcurrent	75A	0.7	IDMT Inverse	75A	0.9	IDMT Inverse
Earth Fault	25A	0.7	Inverse	No Change		
SEF	7A	7s	N/A	No Change		



ID		Plant Description	Model	PSR Status	Set Group	Trip No	Trip Type	Stage No	PickUp	TMS/DT(s)	Curve Type	Minimum Time	Add Time
1		Custom Placeholder (New Custom Pl	RC10-5002-04	Custom	1	1	EF	1	25 A	0.7	Inverse (NOJA)	---	---

Figure 45: Expected operating time for the applied Earth Fault

Figure 46 shows a measured time of 7.1138 seconds (red circle) captured by the injection test set.

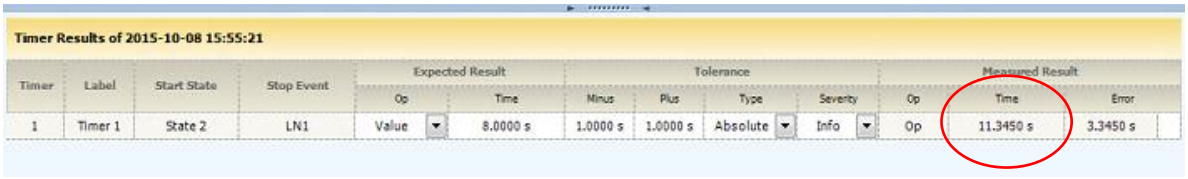


Timer Results of 2015-10-08 15:43:01

Timer	Label	Start State	Stop Event	Expected Result		Tolerance				Measured Result		
				Op	Time	Minus	Plus	Type	Severity	Op	Time	Error
1	Timer 1	State 2	LN1	Value	8.0000 s	1.0000 s	1.0000 s	Absolute	Info	Op	7.1138 s	-0.8862 s

Figure 46: Actual operate time for the applied Earth Fault setting

A second configuration download was performed with changes as listed in the required settings column of Table 9. At the same time the configuration was delivered, a simulated Earth fault of 50A was injected into the Protection IED. The configuration was delivered and took effect before the time characteristic could expire resulting in the operated time being extended. The delay in tripping is shown in Figure 47; increasing the trip time to 11.345 seconds, which imposed an additional delay of 4.322 seconds. As demonstrated the effect of this occurrence is cumulative and as previously discussed and is dependent on when in the timer's cycle the configuration takes effect.



Timer Results of 2015-10-08 15:55:21

Timer	Label	Start State	Stop Event	Expected Result		Tolerance				Measured Result		
				Op	Time	Minus	Plus	Type	Severity	Op	Time	Error
1	Timer 1	State 2	LN1	Value	8.0000 s	1.0000 s	1.0000 s	Absolute	Info	Op	11.3450 s	3.3450 s

Figure 47: Actual delayed tripping time for the applied Earth Fault setting

6.1.7. Mitigation of the exposure to delayed tripping

To try and mitigate or reduce the occurrence of the delay tripping the hierarchy of hazard controls, in Figure 48 were considered.

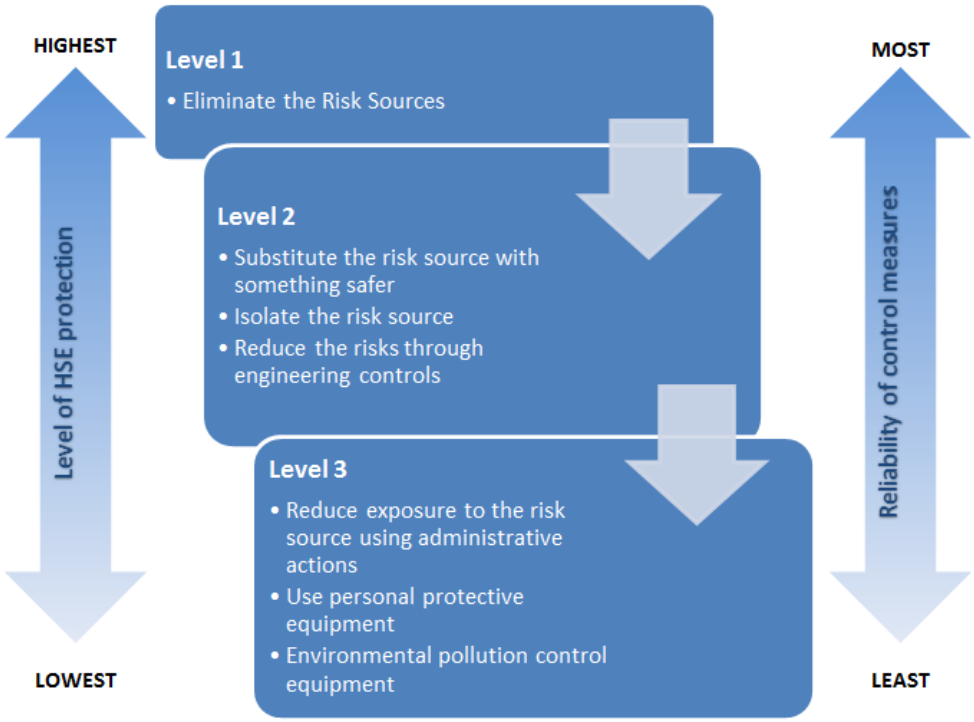


Figure 48: Hierarchy of Hazard Control (Ergon Energy 2010)

The first method considered was to send the proposed configuration file to the Protection IED's setting group 2 (SG2) and when delivery is complete controlled switching is undertaken to switch setting groups (i.e. SG1 to SG2) providing an engineering control to the problem. However this solution would introduce confusion amongst personnel that interact with these devices on a regular basis, owing to the historical processes that maintain setting group (SG1) as the primary setting group. To address any form of confusion, administrative controls would need to be implemented

to prevent setting group 1 (SG1) being inadvertently reinstated. Although this process would be effective to eliminate the delayed tripping at the time of delivery, the operational risk arises again during the switching between groups. It was deemed that the considered control measures would not provide any additional reduction of the risk.

Another considered approach was to examine existing protection elements contained with the protection IED that could be used to accelerate tripping for a network fault. The testing undertaken demonstrated that the time taken to deliver the setting was irrelevant. The delay trip will occur if the new configuration has taken effect at the time a protection timer is running. Implementation of this solution would also require administration controls and was deemed to provide no further benefit.

Elimination of the occurrence would be the preferred result. To obtain such an outcome power utilities will need to engage with Protection IED manufacturers to discuss and promote changes to how a Protection IED responds to online setting changes.

6.2. Chapter Summary

This chapter describes the tests undertaken to evaluate a Basic IED's response to a simulated remote delivery of a configuration file with the testing highlighting the possibility of a delayed tripping occurrence a during network faults. Methods of hazard control to reduce or eliminate the occurrence were discussed including their effectiveness in reducing the hazard.

Chapter 7

Operational Risks

This chapter discusses the operational risks and the level of risk each operational risk imposed onto the distribution network including methods that are recommended to be employed to maintain or reduce risk.

Considered risks associated with the network:

- Device identification
- Delayed tripping
- Inadvertant trip operation
- Communication failures

7.1. Device Identification

Appropriate identification methods are required to ensure that the correct Basic IED requiring modification is being communicated too. Download of a configuration can create the following operational risks;

- Operation of the ACR for normal system conditions- owing to a overcurrent threshold which is too low for the normal load current of the protected feeder.
- Inadequate Protection Reach Factors – an incorrect threshold value has the potential to reduce Protection Reach Factors introducing an unsafe condition for the network during a fault event.

To reduce the occurrence of this happening, it is recommended that the Basic IED's identity should be verified by two persons, which introduces a secondary check procedure (Heggie 2015). To reduce the consequence, the presence of backup protection for the Protection IED under reconfiguration is also recommended. The fault tree depicted in Figure 49, provides the probability for an incorrect connection to the Basic IED. The probability is determined to less than 10% and using Ergon Energy's Risk of Likelihood table (Table 21 Appendix G.3) a category of rare was determined for the event. The consequence category of the event was determined as moderate (Table 22 Appendix G.4); considering backup protection would be employed for an undefined period of time; the level of risk was determined using Table 19 in Appendix G.1 with a summary of the outcome displayed in Table 10.

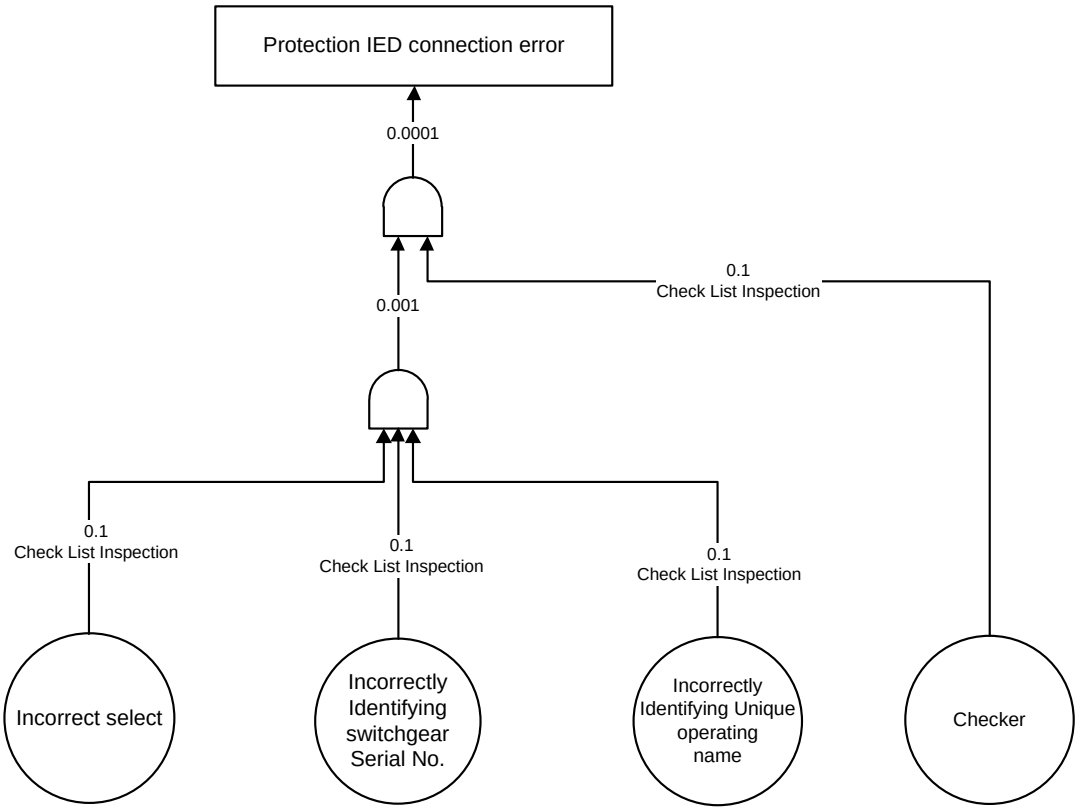


Figure 49: Probability error – Protection IED connection error

Table 10: Level of Risk – correct Protection IED connection

Likelihood	Consequence	Level of Risk
Rare	Moderate	Low

7.2. Delayed Tripping

As discussed in Chapter 6, the possibility of a delayed trip does not introduce any risk of mis-operation; however conductor damage and decreased reliability was are possible impacts imposed on the network for this occurrence.

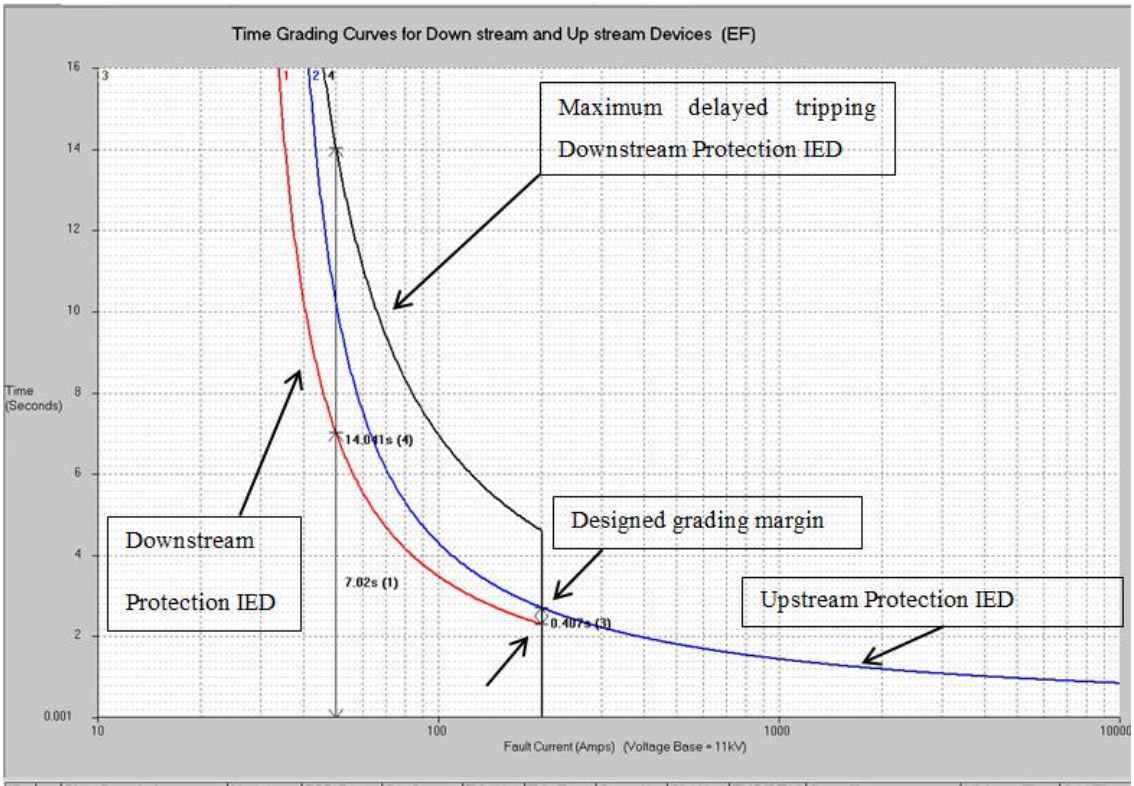
7.2.1. Conductor Damage

As part of the design of an appropriate overcurrent protection characteristic the setter is to consider conductor damage and the cumulative heating effects of automatic reclosing of the ACR. The design requires overcurrent protection to be set with an operating time that does result in conductor heating above the maximum operating temperature that would cause annealing of the conductor. If a delay trip occurs, then one trip cycle of the ACR's auto reclose operation is affected, with either delayed tripping or the fault cleared by the upstream backup protection. As the conductor damage is calculated on the accumulated clearing time, the slower clearing time now becomes part of the accumulated time which was not considered in the original design. However it is considered this occurrence would be similar to that of a circuit breaker fail operation where backup protection would also be required to isolate the fault. Circuit breaker fail, is considered an acceptable network contingency owing to the rare occurrence of circuit breaker fail events.

7.2.2. Decreased Reliability

During delay tripping the reliability of the network can be affected as time grading designed during the setting development stage has been compromised owing to the Basic IED resetting all protection timers. Distribution feeders typically operate with IDMT characteristics due to their radial topology. To provide appropriate fault discrimination along the entire length of the feeder the Basic IED's protection elements are designed with minimum timing margins typically in the order of between 350 – 400 milliseconds. Resetting these timers whilst running compromises these margins and can cause the upstream device to operate; isolating larger portions of network then is required. Figure 50 demonstrates an example of a designed grading margin between the Protection IED under test and an upstream backup protection setting. On detection of the fault both Protection IEDs will initiate their timing elements and owing to the 400

milliseconds grading margin the Protection IED (red curve line) downstream operates before the upstream Protection IED's (blue curve line) timer expires. In cases where the downstream Protection IED does not isolate the fault in time, the upstream Protection IED timer is allowed to expire operating its associated circuit breaker or ACR. The worst case for extended trip time occurs when the new configuration takes affect just prior to the earth fault timer expires; the trip time is now extended by another 7 seconds. The time characteristic (black line) in Figure 50 demonstrates the time is extended to 14 seconds for the worst case.



ID		Plant Description	Model	PSR Status	Set Group	Trip No	Trip Type	Stage No	PickUp	TMS/DT(s)	Curve Type	Minimum Time	Add Time
1		Custom Placeholder (New Custom Pr		Custom	1	1	EF	1	25 A	0.7	Inverse (NOJA)	---	---
							EF	2	200 A	0	DT [100]	---	---
2		Custom Placeholder (New Custom Pr		Custom	1	2	EF	1	30 A	0.75	Inverse (NOJA)	---	---
3		Custom Placeholder (New Custom Pr		Custom	1	3	EF	1	0 A	0	DT [100]	---	---
4		Custom Placeholder (New Custom Pr		Custom	1	4	EF	1	25 A	1.4	Inverse (NOJA)	---	---
		Custom Placeholder (New Custom Pr		Custom	1	4	EF	2	200 A	0	DT [100]	---	---

Figure 50: Demonstrated delay tripping and grading margin between downstream and upstream Protection IEDs

7.2.3. Risk Probability

Testing performed in Chapter 6 confirmed delivering the configuration with a change in protection setting introduces the possibility of delay tripping. The length of delay is dependent on when the new configuration takes effect. If the configuration takes effect whilst a protection timer is half way through its cycle, then the delay tripping will be

increased by approximately half of the timer's value. For delay tripping to occur there needs to be a coincidence of events. The EG-0 Power System Earthing Guide (Energy Networks Association 2010) provides methods of calculating the probability of such events; where the configuration file delivery overlaps the occurrence of a fault event detected on the distribution feeder.

7.2.3.1. Traditional Delivery

Delivery to a configuration at site traditionally requires the ACR to be isolated from the network which entails high voltage switching and isolating the Protection IED to ensure inadvertent tripping does not occur. The procedure is to temporarily replace the ACR's Protection IED with bypass fuses which are incorporated into the design. To perform the bypass, three expulsion dropout fuses are sequentially closed to bypass the ACR. During this operation the Protection IED is blocked to avoid operation of the earth fault protection. Once all three fuses are installed the recloser is opened. On opening of the ACR it becomes isolated form the network and the configuration file is then delivered to the Protection IED. On completion of the works the process is undertaken in reverse to reinstate the ACR to its normal operational state. The procedure prevents an interruption to the customers downstream of the ACR.

ACR Switching times were collected from SCADA and it was possible to identify the time from when the ACR was isolated to the time the ACR was open to complete the works. On average the time taken to complete one operation was 436.5 seconds.

7.2.3.2. Remote Delivery

After pre-delivery checks have been completed (as outlined in section 5.2.2.5) the configuration will be delivered to the remote Protection IED with the ACR's protection remaining in service for the entire process. For the configuration file to take affect the processor has had to acknowledge that the file is complete in its structure. For the IED under test this appeared to be instantaneous, however in calculating the coincidence probability, a conservative time of one second was used.

7.2.3.3. Coincidence Probability

The coincidence probability was calculated for both the remote and the traditional delivery methods to benchmark between the two work practices. Calculations were conducted using the following formula (Energy Networks Association 2010);

$$P_{coinc} = \frac{f_n \times p_n \times (f_d + p_d) \times T}{365 \times 24 \times 60 \times 60} \times CRF \qquad (7.1)^4$$

Where:

p_d is the average duration of the average exposure (in seconds)

f_d is the average duration of the average fault (in seconds)

p_n is the rate at which the exposures occur (exposures or presence/year)

f_n is the rate at which faults occur (faults per year)

T is the number of years (exposure duration) = 1 year

CRF is Coincidence reduction factor (set to 1 normally)

To determine the value for **f_n** the average of faults/100km/year for the Urban, short and long categories for distribution feeders were reviewed. Owing to a higher number of faults recorded the Urban category shown in Table 11 was the worst case scenario. The calculated average for the Urban category was 13.24 faults/100km/year. The mean length of an urban distribution feeder was calculated to be 6.6km (Figure 51) which was used to provide a ratio of events where the mean length was found to less than 100km.

[4] (Energy Networks Association 2010)

Table 11: Distribution feeder length exposure by type (Ergon Energy 2011/2012)

Category	Faults/100km/year				HV km	Line Proportion	Dist Events
	2008/09	2009/10	2010/11	2011/12			
Ergon Energy	4.25	3.94	3.61	4.11	116,079	100%	4,772
Urban	14.87	14.04	12.36	11.69	2,515	2.17%	294
Short Rural	6.90	6.13	6.17	6.19	36,621	31.55%	2,268
Long Rural	2.78	2.53	2.23	2.87	76,943	66.29%	2,210

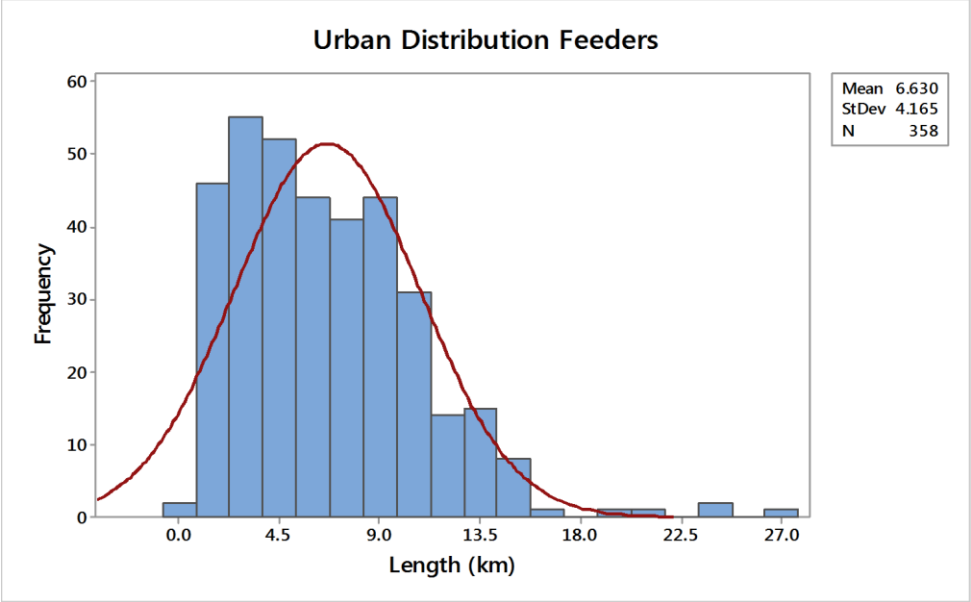


Figure 51: Urban distribution feeder lengths on the Ergon Energy network

Table 12: Values of variables used in calculating Coincidence probability

Variable	Value		Comment
	Traditional	Remote	
p_d	872s	1s	The traditional time was doubled owing to the exposure occurring twice during the delivery process

Variable	Value		Comment
	Traditional	Remote	
$\mathbf{f_d}$	0.2s - 8.0s	0.2s - 8.0s	The probability was plotted over a range of operate times; where 0.2 s is the fastest operate time for a SI IDMT time characteristic typically employed; and 8s which is the longest operate time typically employed for SEF
$\mathbf{p_n}$	1	1	A setting change of once a year was considered
$\mathbf{f_n}$	0.8738 and 3.5748	0.8738 and 3.5748	$f_n = (\frac{13.24}{100}) \times 6.6$ (Avg km feeder length) and $f_n = (\frac{13.24}{100}) \times 27$ (Longest km feeder length)
T	1 year	1 year	(Energy Networks Association 2010)

The coincidence probability for the average urban feeder for both the traditional and remote delivery process were plotted to determine whether the remote delivery operation imposed a higher probability of incidence. As shown in Figure 52 the probability of remote delivery had a lower probability of delay tripping by three orders of magnitude.

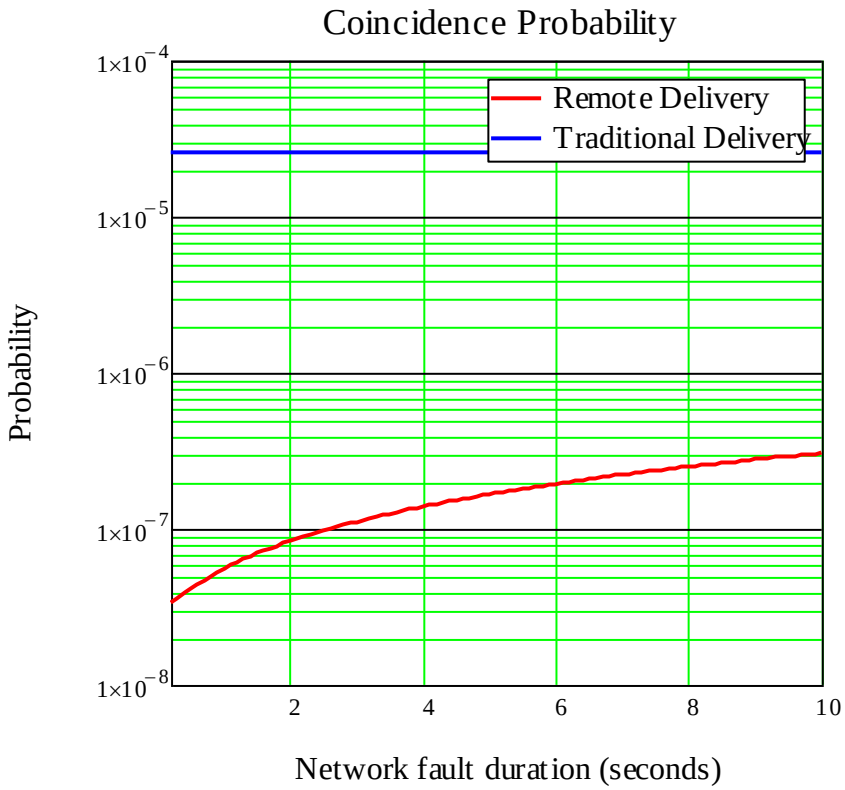


Figure 52: Coincidence probability comparison - average urban feeder length

A second comparison was undertaken to consider the longest urban feeder of 27km (see Figure 51) with the results displayed in Figure 53. It also provided a reduced magnitude of probability; of two to three orders of magnitude.

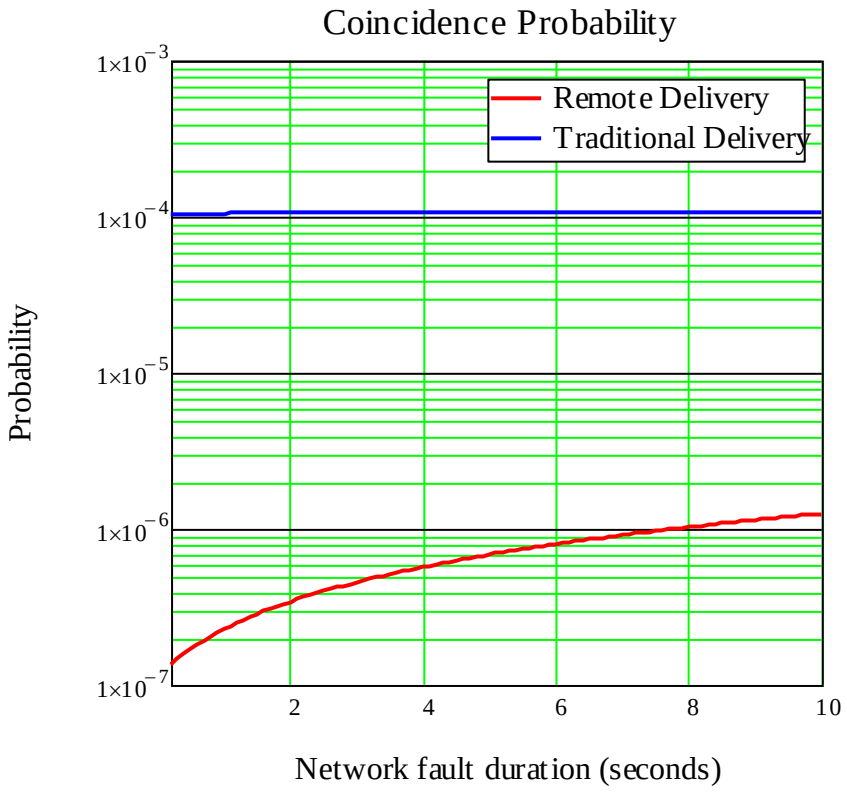


Figure 53: Coincidence probability comparison - longest urban feeder length

The results of these plots identified that the likelihood of a delayed tripping during the remote delivery process was extremely low and imposed no additional adverse effect. These values were aligned with Ergon Energy's Risk of Likelihood table (Table 21 Appendix G.3) to establish a category of likelihood for the occurrence. The consequence was considered minor owing to the network remaining protected throughout the procedure (Table 22 Appendix G.4); with the level of risk determined using Table 19 in Appendix G.1 with a summary of the outcome is displayed in Table 13.

Table 13: Level of Risk - delay tripping occurrence

Likelihood	**Consequence**	**Level of Risk**
Rare	Minor	Very Low

7.3. Inadvertent Trip Operation

The act of writing a configuration file to a Protection IED will not cause a mal-operation (Pingping & Guo 2014) however there is a possibility that an inadvertent trip operation can occur when;

- The designed overcurrent setting threshold is above the load current measured by the Protection IED; typically referred to as a overload trip.
- The ACR's phase sequence is opposite to that configured within the new setting file; and a Negative Phase Sequence (NPS) overcurrent element has been applied for additional backup reach requirements. On delivery of the configuration file the Protection IED would detect NPS current for normal load conditions; and if the standing load was above the NPS current threshold a trip would occur.

The consequence considered for this event was a reduced reliability of supply; impacting on other safety related infrastructure used within the community e.g. traffic lights. The probabilities were aligned with Ergon Energy's Risk of Likelihood table (Table 21 Appendix G.3). The likelihood of this occurrence was deemed to be rare owing to the operational pre-delivery checks undertaken in section 5.2.2.5. The consequence was considered moderate owing to the impact to the reliability of supply (Table 22 Appendix G.4). The level of risk has been determined using Table 19 in Appendix G.1 and a summary of the outcome is displayed in Table 14.

Table 14: Level of Risk - inadvertent trip operation

Likelihood	Consequence	Level of Risk
Rare	Moderate	Low

7.4. Communication Failures

In assessing the operational risks for communication failures four faults have been considered;

- Failure of the computer used to connect and send the configuration file,
- The availability of the communication medium connecting the computer to the device
- Hardware / electrical failure of the equipment used to provide the communication link
- and failure of the Protection IED itself.

The Ergon Energy's Communication Operational Network Centre was contacted to obtain availability figures on communication connectivity between the corporate network and the population of Basic IEDs installed on the distribution network. Figures obtained for the January – March quarter for the connectivity between the communication centre and each Protection IED connected to their prospective 3G modems was calculated to provide a mean availability rate of 98.32% for 1200 Basic IEDs as shown in Figure 54 .

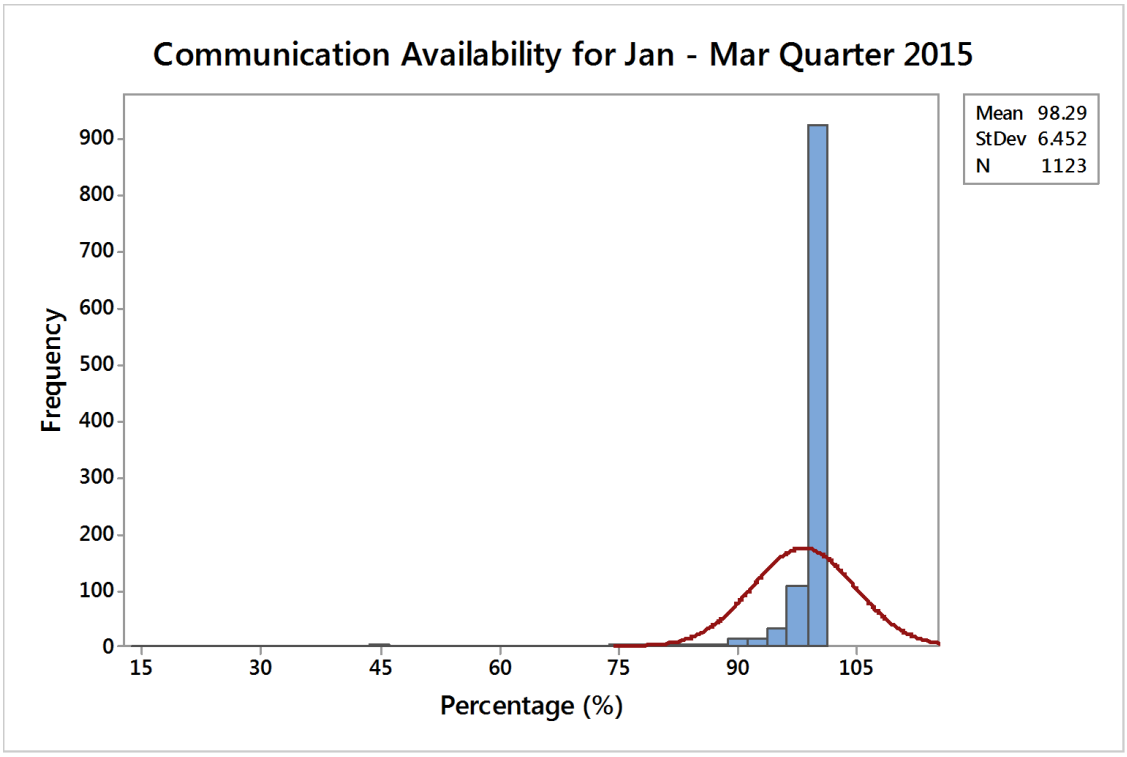


Figure 54: Communication availability for pole mounted Basic IEDs

Although these four faults are probable, the outcomes of communication failure testing described in Chapter 6 resolves them from imposing an operational risk. When a configuration file is being delivered to a Protection IED and a communication failure occurs for any of the four reasons above, testing proved that there would be no ill effect to the Protection IED. The configuration was either received or not received. This was owing to the check process undertaken by the Protection IED prior to the configuration taking effect. Where the remote station is unable to verify the state of the Protection IED in a timely manner then there is a likelihood that the communication module at the ACR has failed. Where this has occurred field crews would be despatched to carry out repairs. When communications become available a remote verification can be undertaken to confirm the state of the configuration.

7.5. Summary of Operation Risks

A summary of the operational risks, their risk rating and control measures recommended are provide in Table 15.

Table 15: Summary of the risk rating for remote configuration delivery

Operational Risk	Risk Rating	Control Measures
Protection IED Identification	Low	• Delivery process as described in section 5.2.2.5
Delayed Tripping	Very Low	• Confirmation backup protection is provided for the reconfigured Basic IED
Inadvertent trip	Low	• Pre-delivery checks as described section 5.2.2.5

7.6. Operational Considerations

Table 16 describes the overview of the how, what, where and why that is recommended to design and create the required checklists, to assist in the decision making for remote delivering of configuration files.

Table 16: Considerations in developing remote delivery checklists

Questions to ask	Requirements to consider
How	The method to deliver remote configuration has been described in Chapter 5 and should be used to maintain the testing and verification requirements needed when a Protection IED is reconfigured remotely.
What	Ergon Energy's Protection Database System currently documents the elements and timers that need to be applied to the Protection IED. The introduction of a remote delivery process will require the ability to record whether the configuration delivery was performed by traditional or remote delivery processes. This will provide a method to track the effectiveness of the delivery process and facilitate continual improvements (Standards Australia 2011).
Where	This is also performed by the existing Protection Database System (PDS) identifying the Protection IED's location on the distribution feeder, including which zone substation it originates from. The location of the Protection IED can also help establish areas where communication connectivity is poor. With this knowledge, decisions can made not to proceed with remote delivery further reducing the possibility of interrupting the verification process failure outlined in Chapter 5.
When	To further reduce any incident of delayed tripping and communication failures, the remote configuration delivery should not be performed during inclement weather (Pingping & Guo 2014) or when programmed works are being undertaken on the distribution feeder associated with the Protection IED.

Questions to ask	Requirements to consider
Why	The ‘why’ is captured in PDS for traditional delivery methods. However a detailed description of the reasons for the change is not mandatory as it is typically described within the Protection setting report. Introduction of any new process requires the ability to analyse, measure and improve the process outcomes. Reportable descriptive details of why the remote configuration was undertaken, has the opportunity to provide valuable information to improve the configuration delivery workflow.
Who	Persons who perform the delivery of configuration files to remote Protection IEDs should be (Standards Australia 2011); • Authorised to peroformed the task • Familiar with the Protection IED, its software and its response to remote configuration • Part of a controlled group within the company to perform such operations.

7.7. Chapter Summary

The chapter identifies the level of risk associated with each consider operational risk in relation to the Basic IED; including control measures to maintain or reduce the exposure. The evaluation of the operational risks highlighted the importance of understanding how the Basic IED responds to remote configuration delivery whilst in service. The learning’s of this chapter will provide the basis for future assessments of other Basic IEDs that require reconfiguring using the same process.

Chapter 8

Feasibility of Remote Configuration

For any organisation a perceived benefit of implementing new processes is there will be efficiency gains through increase productivity and ultimately providing financial benefits. Other reasons power utilities have been reluctant to progress with remote management has been whether the investment would be cost beneficial owing to (CIGRE Working Group B5-09 2006);

- The frequency of setting changes
- Data infrastructure is to expensive where equipment is located in isolated areas and rough terrian.

Since the start of 2015, 153 setting changes have been issued to Ergon Energy field staff to reconfigure Basic IED devices, all of which have connectivity to facilitate remote configuration delivery. As the infrastructure required for the remote management process already exists, the following sections discuss the comparison of the associated costs between the traditional and remote delivery processes, to reconfigure a Basic IED.

8.1. Costs of Traditional delivery

To ascertain the current cost of changing a setting on an ACR installed on Ergon Energy's network a data extraction from the Protection Database System (PDS) was undertaken concentrating on ACRs that were subjected to a reported setting change. The results were then cross referenced with Ergon Energy's works planning database to further categorise the setting changes into the following groups;

- TC – Test and Commission i.e. Capital Works

- MC – Maintenace Corrective i.e Planned works
- MF – Maintenance Forced i.e. Unplannned works

The result returned a total of 818 PSRs issued under the three categories. PSRs issued under a MF category were further analysed owing to these typically requiring immediate action to correct identified issues on the distribution network; prompting a single task being issued to field test staff.

107 PSRs were issued under the Maintenance Forced (MF) category. These 107 were further categorised into actual labour hours taken to complete each task. This returned a range of hours from 0.5 hours – 40 hours. On the premise that a remote change would be expected to take approximately 4 hours, setting changes costed in excess of 8hrs were further analysed. To obtain an average cost for a setting change on ACR, the captured work orders were divided into their allocated 'cost types' of;

- Resource Cost – Labour and Accommodation
- Material Cost – Parts required to perform the task
- Equpment Cost – Vehicle allocation
- Other Cost – Company Overheads

To identify the cost imposed on a daily basis each works order was divided into groups of;

- ≤8 hours
- 12<Actual>8 hours
- 16<Actual>12 hours
- 24<Actual>16 hours

The results are provided in the following figures.

Figure 55 provides the associated costs to complete a setting change on a Basic IED for ≤8 hours.

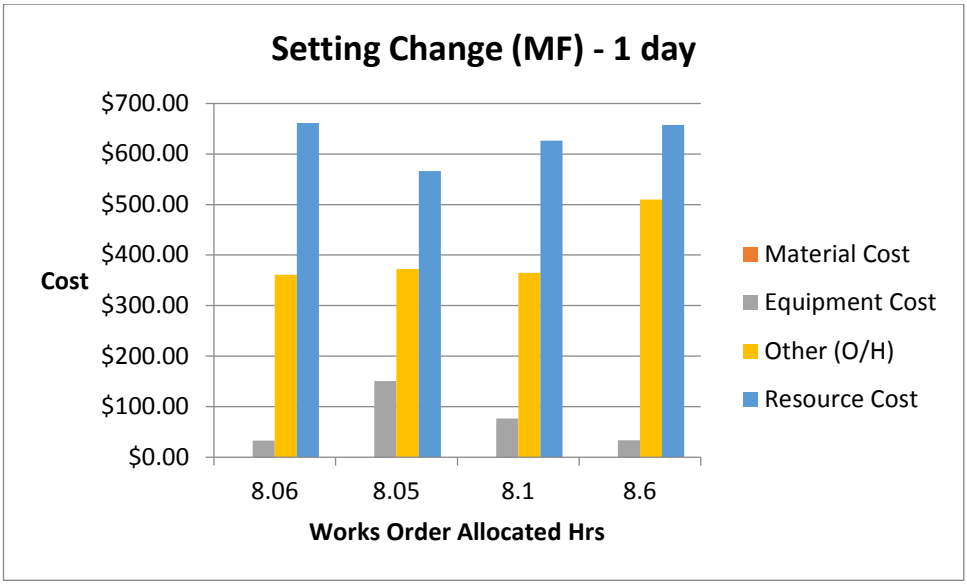


Figure 55: Costs associated with a setting change (MF) – 1 Day

Figure 56 provides the associated costs to complete a setting change on a Basic IED for 12<Actual>8 hours.

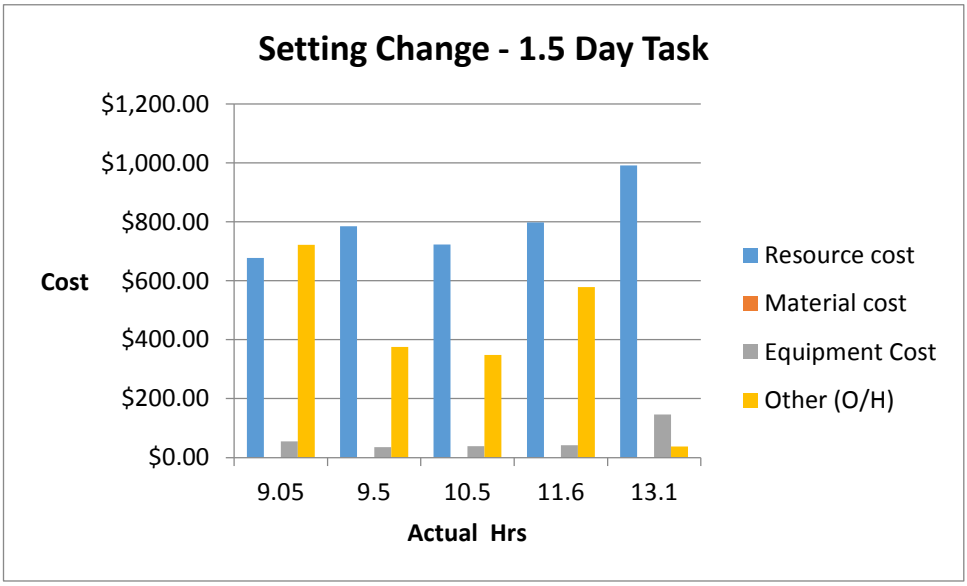


Figure 56: Costs associated with a setting change (MF) – 1.5 Days

Figure 57 provides the associated costs to complete a setting change on a Basic IED for 16<Actual>12 hours.

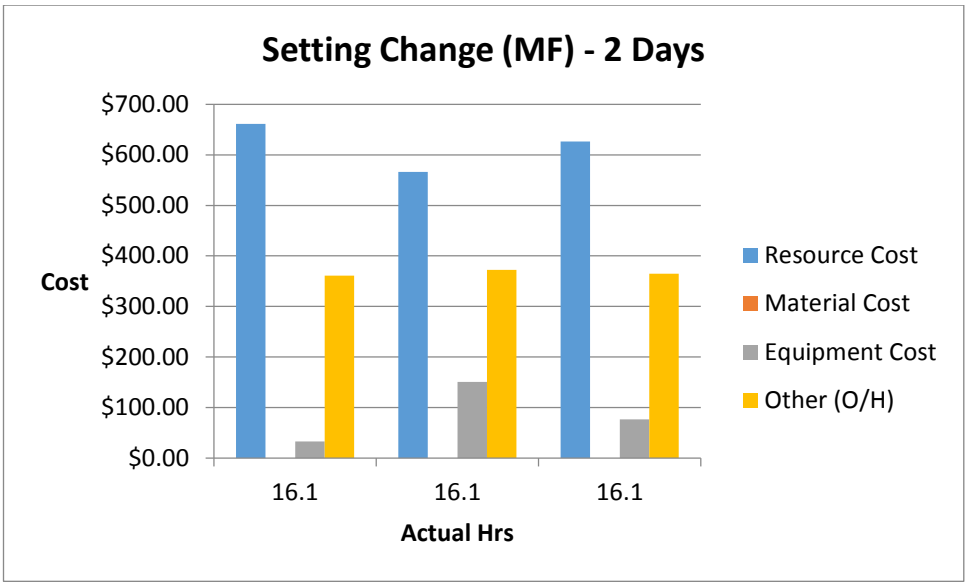


Figure 57: Costs associated with a setting change (MF) – 2 Days

Figure 58 provides the associated costs to complete a setting change on a Basic IED for 24<Actual>16 hours.

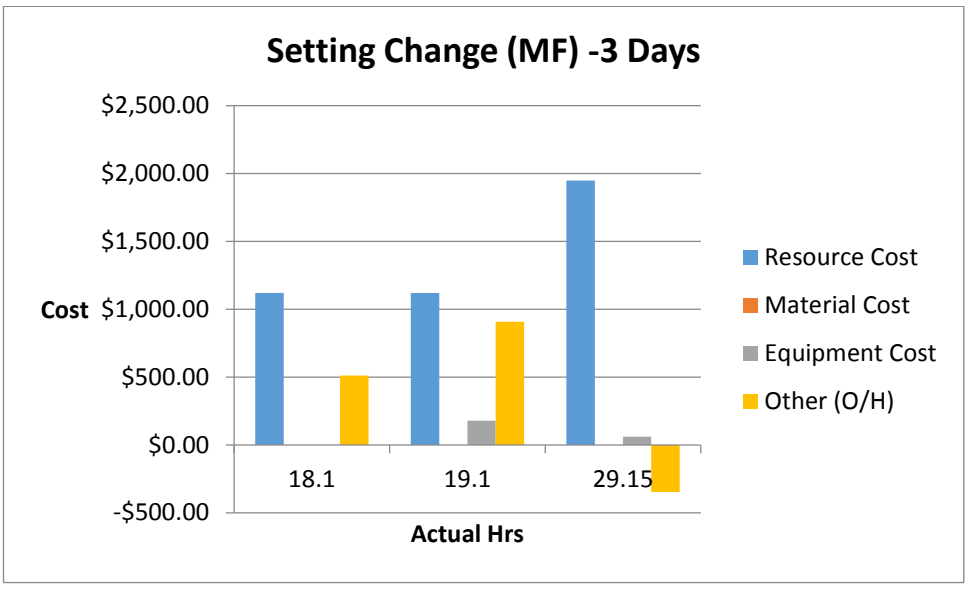


Figure 58: Costs associated with a setting change (MF) – 3 Days

These hours vary across the work undertaken owing to the distance of travel and staff operating under strict fatigue management policies. Some locations can take up two days of travel to arrive at the worksite.

Of the cost types listed, resource and equipment costs are where saving can be made with the introduction of a remote configuration process. Table 17 summarises the average resource and equipment costs associated with each allotted group. The average of the results presented in Table 17 equates to an average cost of $954 ≈ $1000.00 and on average 13.5 man hours to change a setting on an ACR.

Table 17: Summary of costs for allotted groups

Day/s	Average Hours	Average Resource Cost	Average Equipment Cost	Average Total Cost (Resource and Equipment Costs Combined)
1	8.2	$627.00	$73.00	$700.00
1.5	10.75	$795.00	$146.00	$941.00
2	16.10	$618.00	$86.00	$704.00
3	22.0	$1395.00	$79.00	$1474.00

8.2. Cost of Remote delivery

The process outlined in section 5.2 describes a new method of configuration delivery to the Basic IED incorporating laboratory testing and remote delivery of the configuration file. It is proposed field test technicians would be used to test and deliver the configurations. The expected time to perform a setting change on a Basic IED is expected to take approximately 4 hours, equating to a labour cost of $208.00. Comparing this value with the average cost of the traditional delivery provides the opportunity to reduce the delivery cost by approximately 80%.

The recent installation of 487 ACRs under a reliability project further highlights the potential for significant cost savings. Owing to the short installation time frame of these pole mounted Protection IEDs, 244 of these units have been installed as Load Break Switches (LBSs) with a future expectation to be reconfigured to ACRs. Exercising the existing process in section 5.1 to reconfigure these units would be at cost of $232,776.00 compared to $50,752.00 using the process described in section 5.2.

8.3. Chapter Summary

The chapter identifies the cost of using traditional delivery methods to reconfigure the Basic IED type devices and provided a comparison between it and the proposed remote configuration delivery process against future reconfiguring of installed Automatic Reclosers (ACRs). The results demonstrated opportunities of improved cost efficiencies with progressing with a remote configuration management strategy.

Chapter 9

Conclusions & Further Work

9.1. Conclusions

The main objective of the project presented in this dissertation was to determine whether a remote configuration management process could be developed to reduce on-site commissioning and operational works on the existing population of Protection IEDs installed on the Ergon Energy network. By the use of the defined processes it was determined configuration files can be remotely delivered to a selected Basic IED whilst it remains in service, without imposing an increase in operational risks to the distribution network.

In addition to the main objective, a number of other objectives were set and achieved.

These included:

- Analysing Ergon Energy's existing configuration workflow to firstly determine its effectiveness in delivering an error free configuration, and secondly identify where improvements could be made,
- Examination of benchmarking techniques, frequency and magnitude changes that could be used to verify proposed protection settings,
- Recommendations to improve the existing workflow,
- Understand the operational risks associated with remote configuration delivery by testing the response of a selected Protection IED during a simulated delivery.

Improvements to the existing workflow were achieved by implementing targeted checklists and mandatory testing of non-standard functional logic which collectively theoretically reduced discrepancies in configuration files exiting the Protection Setting workflow. To assess whether these suggested improvements are successful the recommended checklists will need to be implemented and the output of the workflow measured and compared against the error values discussed in section 4.4.

The assessment of the alternate verification process against the prescribed legislative, regulatory and Ergon Energy standards did not identify non-compliance towards the requirements of testing installed Protection IEDs. Furthermore assessment against traditional delivery methods found the alternate process to be more robust in its ability to verify successful deliveries of configuration files. Future implementation of the proposed remote delivery process also identified opportunities to improve operational efficiencies providing opportunities to reduce Ergon Energy's operational expenditure (OPEX).

Collectively the objectives provide the knowledge and understanding to progress further development of a remote configuration strategy for Basic IEDs installed on a distribution network.

9.2. Further Work

Owing to time constraints it was not possible to investigate or implement all areas identified at the commencement and during the project. These areas have been identified as future works to internally progress remote configuration management of Basic and Intermediate Protection IEDs installed on Ergon Energy distribution network.

These areas include:

1) Deliver the findings of the project to Ergon Energy management and relevant stakeholders to discuss the project findings.
2) Develop and publish the LAB documentation as described in Chapter 5 and commence trails testing and verifying new configuration files to assess the process

3) Implement recommendations to improve the Protection Setting workflow and continue to monitor the progressive survey to measure the improved output.
4) Further investigation into the responses and operational risks of remote configuration delivery where a proposed configuration file intends to impose a change in protection application; concentrating on reconfiguring installed LBSs to ACRs.

The following are area of further work may be investigated by other students;

5) Further development and assessment to determine whether the processes can be expanded to functional logic changes and the additional identifying requirements around the verification process.

References

AEMC - Australian Energy Market Corporation 2014, *National Electricity Rules, Version 65*, viewed 25 October 2014, <http://www.aemc.gov.au/Energy-Rules/National-electricity-rules/Current-Rules>.

Apostolov, A, Tholomier, D & Richards, S 2005, 'Simplifying the configuration of multifunctional protection relays', *58th Annual Conference for Protective Relay Engineers* , <http://ieeexplore.ieee.org.ezproxy.usq.edu.au/>.

Bian, JJ, Slone, AD & Tatro, PJ 2014, 'Protection system misoperation analysis ', *PES General Meeting | Conference & Exposition, IEEE*.

CIGRE Study Committee B5-205 2014, *Remote system & change management of substation automation systems*, <http://www.e-cigre.org/Search/Ru_se.asp>.

CIGRE Working Group 34.10 2000, *CIGRE Analysis and Guidelines for Testing Numerical Protection Schemes*, viewed 15 October 2014, <http://www.e-cigre.org/Search/Ru_se.asp>.

CIGRE Working Group B5.27 2013, *CIGRE - Implications and benefits of standardised protection schemes*, viewed 28 October 2014, <http://www.e-cigre.org/Search/Ru_se.asp>.

CIGRE Working Group B5.31 2013, *CIGRE , Life-time Management of Relay Settings*, viewed 23 October 2014, <http://www.e-cigre.org/Search/Ru_se.asp>.

CIGRE Working Group B5-09 2006, *Remote On-line Management for Protection and Automation*, viewed 2014 October 2014, <http://www.e-cigre.org/Search/Ru_se.asp>.

CIGRE Working Group B5-27 2014, *CIGRE Session B5, Implications and Benefits of Standardised Protection and Control Schemes*, viewed 29 October 2014, <http://www.e-cigre.org/Search/Ru_se.asp>.

CIGRE Working Group B5-51 2008, *Methods and application of remotely accessed information for SAS maintenance and operation*, viewed 25 October 2014, <http://www.e-cigre.org/Search/Ru_se.asp>.

Electricity Act, Queensland, 1994, *Electricity Act, Queensland, 1994*, viewed 25 October 2014, <https://www.legislation.qld.gov.au>.

Energy Networks Association 2010, *EG-0 Power System Earthing Guide Part1: Management Principles Version 1*, Barton, ACT.

Engineering Australia 2012, *Risk & Liability Management: Engineering Due Diligence*, 2nd edn, Engineering Educaion Australia, EEA, Melbourne.

Ergon Energy 2004, 'Protection Setting Development and Delivery Procedure', Network Assests, Ergon Energy, Queensland.

Ergon Energy 2010, 'Hazard, Risk and Change Management Reference', Ergon Energy, Queensland.

Ergon Energy 2011/2012, 'Annual Network Reliability Performance Report', Network Reliability team, Ergon Energy, Queensland.

Ergon Energy 2012, *Protection Relay Testing for Commissioning SWP*, Queensland, viewed 12 May 2015, <https://www.ergon.com.au/__data/assets/pdf_file/0003/146271/SP0518.pdf>.

Ergon Energy 2012, 'STNW1156 - Maintenance Standard: Standard for Protection and Control Systems', Maintenance Standards, Ergon Energy, Queensland.

Ergon Energy 2013, 'Coporate Risk Assessment Tables', Ergon Energy, Queensland.

Ergon Energy 2014, 'STNW1002 Standard for Substation Protection', Substation Standards, Ergon Energy, Queensland.

Ergon Energy/Energex 2010, 'Standards for Protection Systems', Maintenance Standard, Queensland.

Haimes, YY 2009, *Risk Modelling, Assessment, and Management*, 3rd edn, A JOHN WILEY &SONS, Hoboken, New Jersey.

Heggie, G 2015, ' Remote Setting Changes', *SEAPAC*, Sydney.

Hopkins, A 2000, *Lessons From Longford; The Esso Gas Plant Explosion.*, 1st edn, CCH Australia Limited, Australia.

Kezunovic, M 2002, *Future Trends in Protective Relaying, Substation Automation, Testing and Related Standardization, Transmission and Distribution Conference and Exhibition 2002: Asia Pacific. IEEE/PES*, viewed 24 October 2014.

Kjolle, GH 2002, 'Fault Statistics as a Basis for Designing Cost-effective Protection and Control Solutions', 34-103, CIGRE.

Kumm, JJ, Schweitzer, EO & Hou, D 1995, 'Assessing the Effectiveness of Self-Tests and Other Monitoring Means in Protective Relays', *1995 Pennsylvania Electric Association Relay Committee Spring Meeting*, Matamoras, Pennsylvania.

Liang, GF, Lin, JT, Wang, EMY & Patterson, P 2010, 'Preventing human errors in aviation maintenance using an on-line maintenance assistance platform', *International Journal of Industrial Economics*, pp. 356-367.

Musaruddin, M, Zaporoshenko, M & Zivanovic, R 2008, 'Remote Protective Relay Testing', *AUPEC, Australasian Universities Power Engineering Conference*, viewed 25 October 2014, <http://scholar.google.com.au/scholar?q=Remote+Protective+Relay+Testing&btnG=&hl=en&as_sdt=0%2C5>.

Pingping, D & Guo, J 2014, 'The research on safe reliability of remote control system of relay protection device ', *2014 IEEE Workshop on Advanced Research and Technology in Industry Applications (WARTIA)*.

Queensland Government 2006, *Electricity Regulation, Queensland, 2006*, viewed 27 October 2014, <https://www.legislation.qld.gov.au>.

Queensland Government 2013, *Electricity safety code of practice*, viewed 31 October 2014, <http://www.justice.qld.gov.au/__data/assets/pdf_file/0015/25404/es-code-of-practice-risk-management.pdf>.

Siu, N 1994, 'Risk assessment for dynamic systems: an overview. Reliability engineering & system safety', pp. 43-73, viewed 2014 October 2014.

Stamatelatos, M, *NASA Office of Safety and Mission Assurance. Probabilistic Risk Assessment: What Is It And Why Is It Worth Performing It?, viewed 27 October 2014.*, viewed 27 Ocrober 2014, <http://www.hq.nasa.gov/office/codeq/qnews/pra.pdf>.

Standards Australia 2011, 'AS61508.1 2nd edition: Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 1: General requirements'.

Standards Australia 2011, 'AS61508.3, Second edition: Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 3: Software requirements'.

Standards Australia 2014, 'Draft for Public Comment DR AS 2067:2014', Standards Australia.

Working Group B5.09 2006, 'Remote On-Line Management for Protection and Automation', Technical brochure, CIGRE.

Zimmerman, K 2014, 'SEL Recommendations on Periodic Maintenance Testing of Protective Relays', White Paper, Illinois.

Appendix A Project Specification

Topic: Remote Management of Safety Systems in Power Utility Installations

Supervisor: Dr Leslie Bowtell BEng, MEng, PhD *USQ*

Rob Coggan, Engineering Manager Substations Standards, Ergon Energy (Industry Supervisor)

Sponsor: Ergon Energy

Project Aim: The aim of this project is to investigate the systems, processes and design criteria that will facilitate remote management of protection and control infrastructure used within Power Utilities.

Programme:

(Version B, 24 September, 2015)

1) Identify existing work flows of Ergon Energy's current configuration development and research the effectiveness of current management strategies through analysis of survey and internal non-conformance logs

2) Investigate methods for setting verification

3) Design a new IED configuration delivery process and analyse its efficiency and effectiveness against existing processes established in (1).

4) Research and evaluate an alternate method to support remote configuration verification of selected protection IEDs used on the Ergon Energy network.

5) Research and test how selected IEDs respond to configuration delivery whilst remaining in service.

6) Development of risk matrix to be used for remote configuration delivery

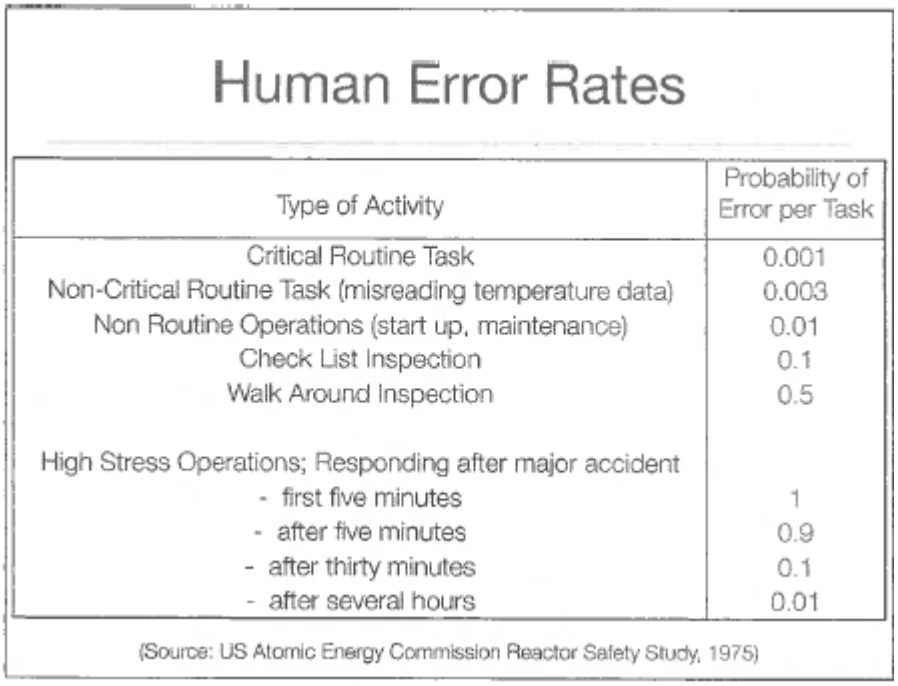
As time permits:

7) Introduce the improved configuration management process into Ergon Energy's protection design work flow for selected IEDs and progressively resurvey the same staff to evaluate the new workflow.

Appendix B: Probability Tables

B.1 Probability Error Rates

The following tables were used to apply errors of probability to the fault tree analysis described in Chapter 4 (Engineering Australia 2012).

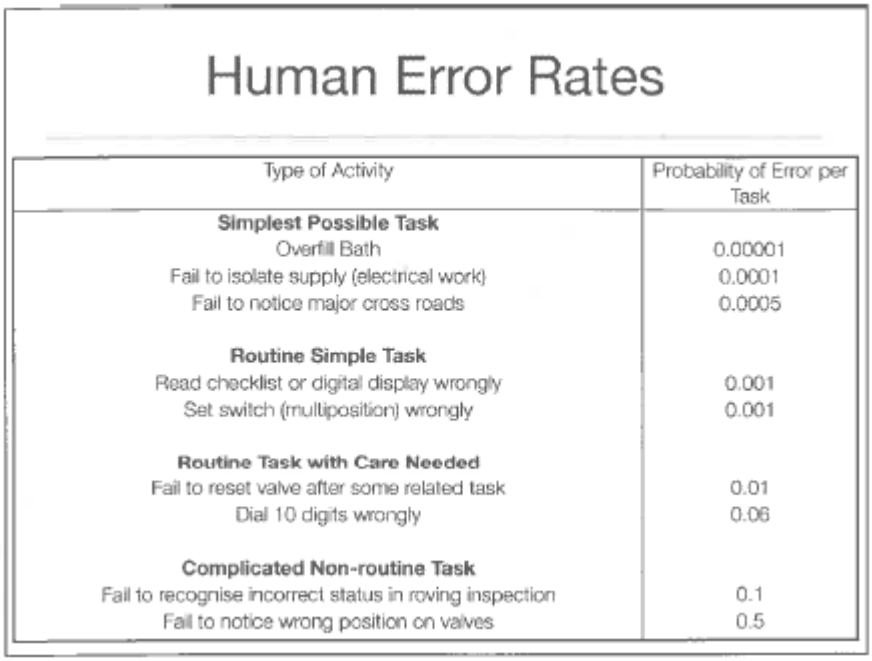


Human Error Rates

Type of Activity	Probability of Error per Task
Critical Routine Task	0.001
Non-Critical Routine Task (misreading temperature data)	0.003
Non Routine Operations (start up, maintenance)	0.01
Check List Inspection	0.1
Walk Around Inspection	0.5
High Stress Operations; Responding after major accident	
- first five minutes	1
- after five minutes	0.9
- after thirty minutes	0.1
- after several hours	0.01

(Source: US Atomic Energy Commission Reactor Safety Study, 1975)

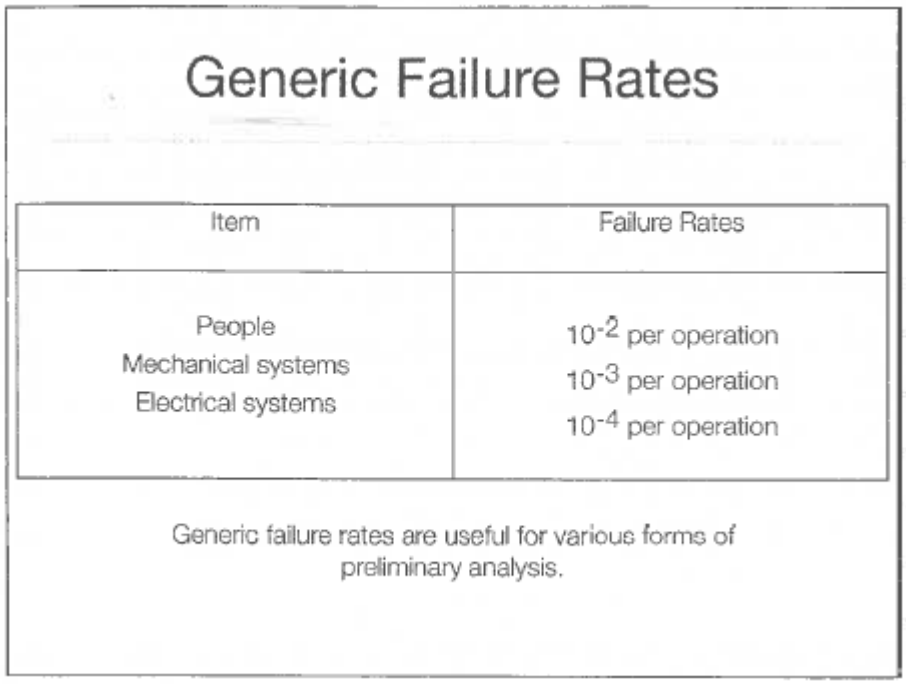
Figure 59: Probability of human error rates -1



Human Error Rates

Type of Activity	Probability of Error per Task
Simplest Possible Task	
Overfill Bath	0.00001
Fail to isolate supply (electrical work)	0.0001
Fail to notice major cross roads	0.0005
Routine Simple Task	
Read checklist or digital display wrongly	0.001
Set switch (multiposition) wrongly	0.001
Routine Task with Care Needed	
Fail to reset valve after some related task	0.01
Dial 10 digits wrongly	0.06
Complicated Non-routine Task	
Fail to recognise incorrect status in roving inspection	0.1
Fail to notice wrong position on valves	0.5

Figure 60: Probability of human error rates -2

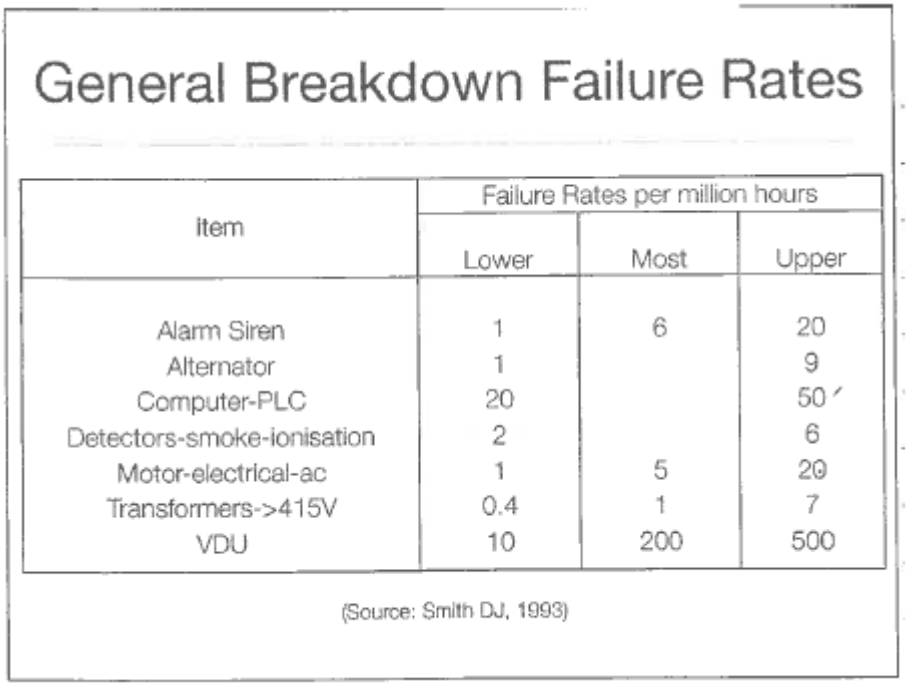


Generic Failure Rates

Item	Failure Rates
People	10^{-2} per operation
Mechanical systems	10^{-3} per operation
Electrical systems	10^{-4} per operation

Generic failure rates are useful for various forms of preliminary analysis.

Figure 61: Probability of generic failure rates



General Breakdown Failure Rates

Item	Failure Rates per million hours		
	Lower	Most	Upper
Alarm Siren	1	6	20
Alternator	1		9
Computer-PLC	20		50
Detectors-smoke-ionisation	2		6
Motor-electrical-ac	1	5	20
Transformers->415V	0.4	1	7
VDU	10	200	500

(Source: Smith DJ, 1993)

Figure 62: Probability of general breakdown failure rates

Appendix C: Survey Questions and Results

Survey questions developed and delivered to Ergon Energy's Field Test Staff are listed in section Appendix C. The respondents were asked to rank the 'origin' and 'type of error' for each feature they had deemed to have a discrepancy. The results of the more granular questions are displayed in section C.3.

C.1 Perception Survey Questionnaire

Relay Configuration Management - Field Test

General Information

This Survey seeks to provide the Protection Standards group with an overview of protection relay configuration errors of the past 6 months. The information will be used to help identify deficiencies in the current configuration management process with a goal to limit the amount of rework required during installation.

For the purpose of this survey two types of IEDS shall be considered;

BASIC - Variable tripping characteristics and fixed functionality (e.g. pole mounted automatic reclosers, sectionalisers)

INTERMEDIATE - Variable tripping characteristics and configure functionality and I/O (e.g. Feeder management, transformer differential relays)

* 1. Please select your region of work?

- ◯ FN
- ◯ NQ
- ◯ MK
- ◯ CA
- ◯ WB
- ◯ SW
- ◯ Banyo Workshops

* 2. Please select the number of years you have been in the role as a test technician within Ergon Energy?

- ◯ 1 to 3
- ◯ 3 to 5
- ◯ 5 to 7
- ◯ 7 to 9
- ◯ Other (please specify a number)

1

* 3. Over the last 6 months on average how many IEDs (Intelligent Electronic Devices) would you have commissioned per month (Please consider a month to be 20 working days)?

- ◯ 2 to 6
- ◯ 6 to 10
- ◯ 10 to 14
- ◯ 14 to 18
- ◯ 18 to 22

* 4. Over the last 6 months on average how many IEDs (Intelligent Electronic Devices) would you have maintained per month (Please consider a month to be 20 working days)?

- ◯ 2 to 6
- ◯ 6 to 10
- ◯ 10 to 14
- ◯ 14 to 18
- ◯ 18 to 22

Relay Configuration Management - Field Test

Basic IED

* 5. Over the last 6 months on average how many Basic IEDs would you have commissioned per month (Please consider a month to be 20 working days)?

- ◯ 2 to 6
- ◯ 6 to 10
- ◯ 10 to 14
- ◯ 14 to 18
- ◯ 18 to 22

* 6. On average; for how many of these devices have you identified an error/s in the device configuration?

- ◯ 1 to 3
- ◯ 3 to 5
- ◯ 5 to 7
- ◯ 7 to 9
- ◯ None
- ◯ Other (please specify a number)

* 7. Over the last 6 months on average how many Basic IEDs would you have maintained per month (Please consider a month to be 20 working days)?

- ◯ 2 to 6
- ◯ 6 to 10
- ◯ 10 to 14
- ◯ 14 to 18
- ◯ 18 to 22

* 8. On average; for how many of these devices have you identified an error/s in the device configuration?

- ◯ 1 to 3
- ◯ 3 to 5
- ◯ 5 to 7
- ◯ 7 to 9
- ◯ None
- ◯ Other (please specify a number)

* 9. If you have answered 'None' above for identified errors for both commissioned and maintained IEDs please select 'No Errors'. Otherwise please select 'Continue'

- ◯ No Errors
- ◯ Continue

4

Relay Configuration Management - Field Test

This section considers the frequency of the type of errors encountered.

* 10. In consideration of the Basic IED configurations you have 'worked with' over the past 6 months that you deem to have contained one or more errors please rank the frequency of each error type.

	Error not observed or Unsure	Error rarely observed	Error sometimes observed	Error regularly observed	Error always observed
Tripping Threshold	○	○	○	○	○
Time characteristic	○	○	○	○	○
Control or Indication	○	○	○	○	○
Device firmware	○	○	○	○	○

* 11. Of these device configurations that have been corrected and re-issued to you please rank the occurrence of the device configuration still containing error/s;

- ○ Never or Unsure
- ○ Rarely
- ○ Sometimes
- ○ Usually
- ○ Always

* 12. Please rank the occurrence of repeated error/s i.e. the error/s initially identified remained in the re-issued device configuration;

- ○ Never or Unsure
- ○ Rarely
- ○ Sometimes
- ○ Usually
- ○ Always

* 13. In consideration of possible 'Tripping threshold' errors are you willing to provide more information?

- ○ Yes
- ○ No

Relay Configuration Management - Field Test

Basic IED Configuration Error

* 14. In consideration of possible 'Time characteristic' errors are you willing to provide more information?

- ◯ Yes
- ◯ No

6

Relay Configuration Management - Field Test

Basic IED Configuration Error

* 15. In consideration of possible 'Control and Indication' errors are you willing to provide more information?

- ◯ Yes
- ◯ No

7

Relay Configuration Management - Field Test

Basic IED Configuration Error

* 16. In consideration of possible 'Device firmware' errors are you willing to provide more information?

- ◯ Yes
- ◯ No

8

Relay Configuration Management - Field Test

Basic IED Configuration Error

* 17. Are there other device configuration error types not already mentioned that you have identified over the past 6 months?

- ◯ Yes
- ◯ No

9

Relay Configuration Management - Field Test

Tripping Threshold Error (Basic IED)

* 18. Please rank the 'origin' of threshold error in order of occurrence, where '1' is the highest;

- [ ] PSR (Protection Setting Request)
- [ ] Protection setting report
- [ ] Configuration File

* 19. Please rank the 'type of error' in order of occurrence, where '1' is the highest;

- [ ] Invalid Setting e.g. Protection device unable to accept value or out of range value
- [ ] Incorrect threshold value
- [ ] Incorrect element selection

* 20. On average what was the estimated time taken to rectify the error?

- ( ) <4 hours
- ( ) 8 hours
- ( ) 16 hours
- ( ) 40 hours
- ( ) Other (please specify a number in hours)

10

Relay Configuration Management - Field Test

Time Characteristic Error (Basic IED)

* 21. Please rank the 'origin' of time characteristic error in order of occurrence, where '1' is the highest;

- [ ] PSR (Protection Setting Request)
- [ ] Protection setting report
- [ ] Configuration file

* 22. Please rank the 'type of error' in order of occurrence, where '1' is the highest;

- [ ] Invalid Setting e.g. Protection device unable to accept value or out of range value
- [ ] Incorrect time characteristic
- [ ] Incorrect timer selection

* 23. On average what was the estimated time taken to rectify the error?

- ◯ <4 hours
- ◯ 8 hours
- ◯ 16 hours
- ◯ 40 hours
- ◯ Other (please specify a number in hours)

11

Relay Configuration Management - Field Test

Control or Indication Error (Basic IED)

* 24. Please rank the 'origin' of Control or indication error in order of occurrence, where '1' is the highest;

- [ ] Protection setting report
- [ ] Configuration File
- [ ] SCADA configuration

* 25. Please rank the 'type of error' in order of occurrence, where '1' is the highest;

- [ ] LEDs incorrectly configured
- [ ] Device Control incorrectly configured
- [ ] Incorrect Binary point/s
- [ ] Incorrect Analogue Point/s
- [ ] Event recorder incorrectly configured

* 26. On average what was the estimated time taken to rectify the error?

- ◯ <4 hours
- ◯ 8 hours
- ◯ 16 hours
- ◯ 40 hours
- ◯ Other (please specify a number in hours)

12

Relay Configuration Management - Field Test

Firmware Error (Basic IED)

* 27. Please rank the 'origin' of firmware error in order of occurrence, where '1' is the highest;

- [ ] PSR (Protection Setting Request)
- [ ] Configuration file
- [ ] Vendor software

* 28. Please rank the 'type of error' in order of occurrence, where '1' is the highest;

- [ ] Configuration file incompatibility
- [ ] Protection device incompatibility
- [ ] Issued firmware version incorrect
- [ ] Field Test PC incompatibility

* 29. On average what was the estimated time taken to rectify the error?

- ◯ <4 hours
- ◯ 8 hours
- ◯ 16 hours
- ◯ 40 hours
- ◯ Other (please specify a number in hours)

13

Relay Configuration Management - Field Test

Other Errors (Basic IED)

* 30. Please enter a short description of error and example

14

C.2 Progressive Survey Questionnaire

Device Configuration Errors - Field Test

General Information

This Survey is to be used to capture errors or discrepancies found with a relay configuration during either commissioning or maintenance works.The information will be used to help identify deficiencies in the current configuration management process with a goal to limit the amount of rework required during device configuration application.

1. Please Select your region of work

- ○ HN
- ○ NQ
- ○ MK
- ○ CA
- ○ WB
- ○ SW
- ○ Banyo

* 2. Please enter the works order issued to undertake the work;

* 3. Please enter your Name (used to enable contact for further details)

4. Were there discrepancies identified with this task?

- ○ Yes
- ○ No

1

Device Configuration Errors - Field Test

Information on Discrepency

* 5. Please select the work that was undertaken;

- ◯ Commissioning - Brown Field
- ◯ Commissioning - Green Field
- ◯ Corrective Maintenance
- ◯ Preventative Maintenance

* 6. Please select the device type deemed to have error/s?

- ◯ Basic IED (e.g. Recloser, Sectionaliser)
- ◯ Intermediate IED (e.g. Feeder management relay, Transformer differential relay)
- ◯ Integrated IED (e.g. Line Differential or Comms Assisted Distance)

* 7. Please select the device configuration error/s type found;

- ☐ Threshold value
- ☐ Time characteristic
- ☐ Logic Operation/Functionality
- ☐ Control and/or Indication
- ☐ Device firmware
- ☐ Functional Design

Other (please provide a brief description)

* 8. Please select the estimated time taken to rectify the error?

- ◯ <1 hours
- ◯ 8 hours
- ◯ 16 hours
- ◯ 40 hours
- ◯ Other (please specify a number in hours)

2

* 9. If a device configuration was deem to have error/s was it:

	Yes	No
Re-issued still containing error/s	○	○
Re-issued with repeated error/s	○	○

3

Device Configuration Errors - Field Test

End of Survey

This concludes the survey and thank-you for responding. If you wish to provide any additional comments regarding the task undertaken please provide comments below.

10. Comments

C.3 Perception Survey Results

C.3.1 Origin and Type of Errors for Tripping Threshold

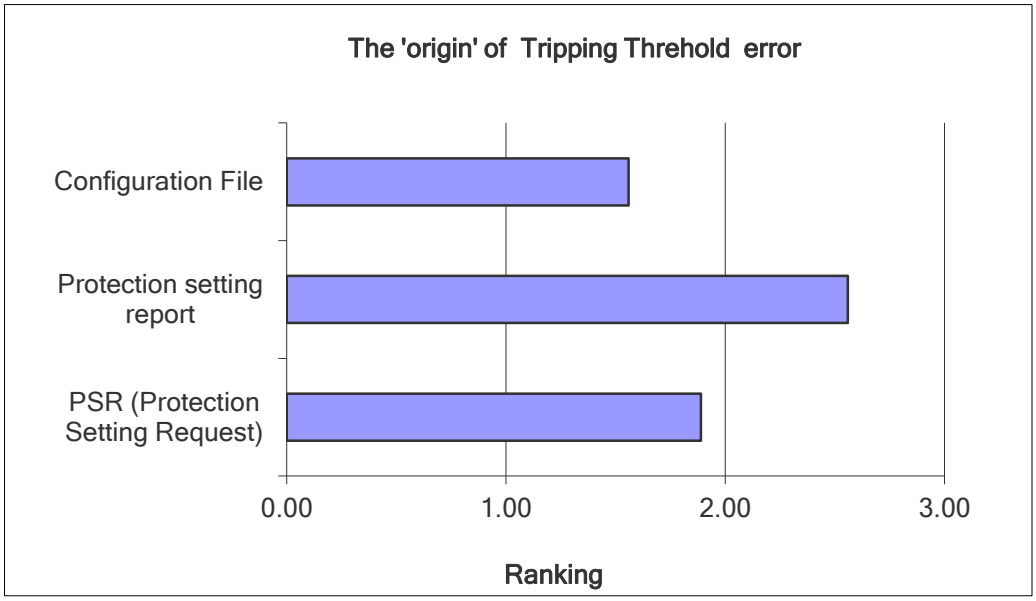


Figure 63: Perception Survey - The 'origin' of Tripping Threshold errors

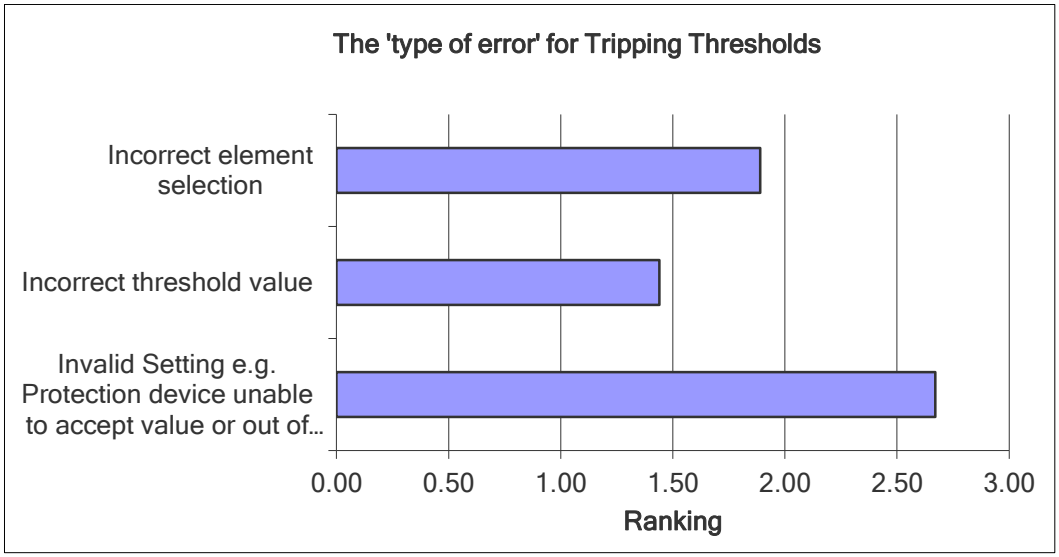


Figure 64: Perception Survey - The 'type of error' for Tripping Thresholds

C.3.2 Origin and Type of Errors for Time Characteristics

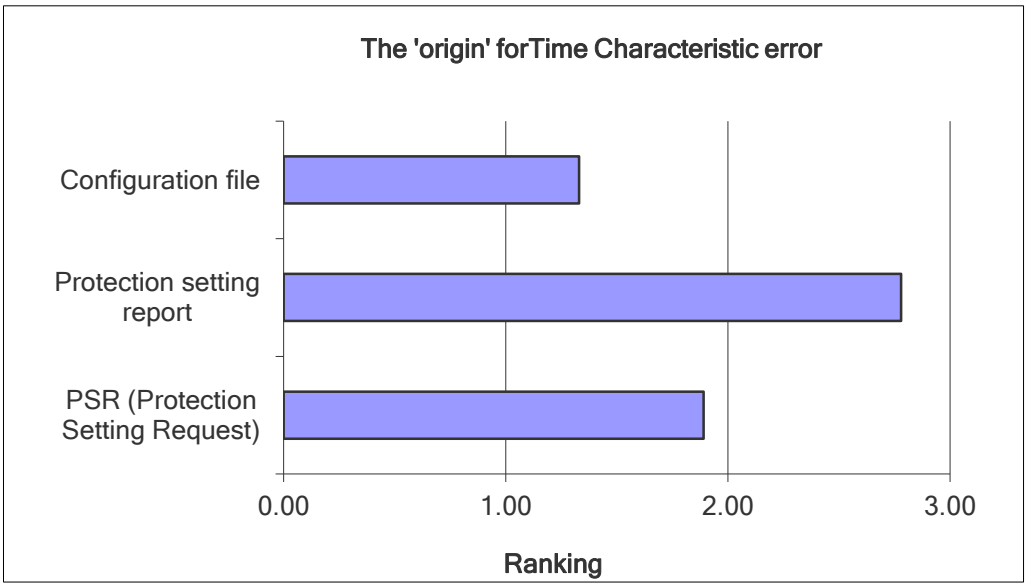


Figure 65: Perception Survey - The 'origin' of Time Characteristic errors

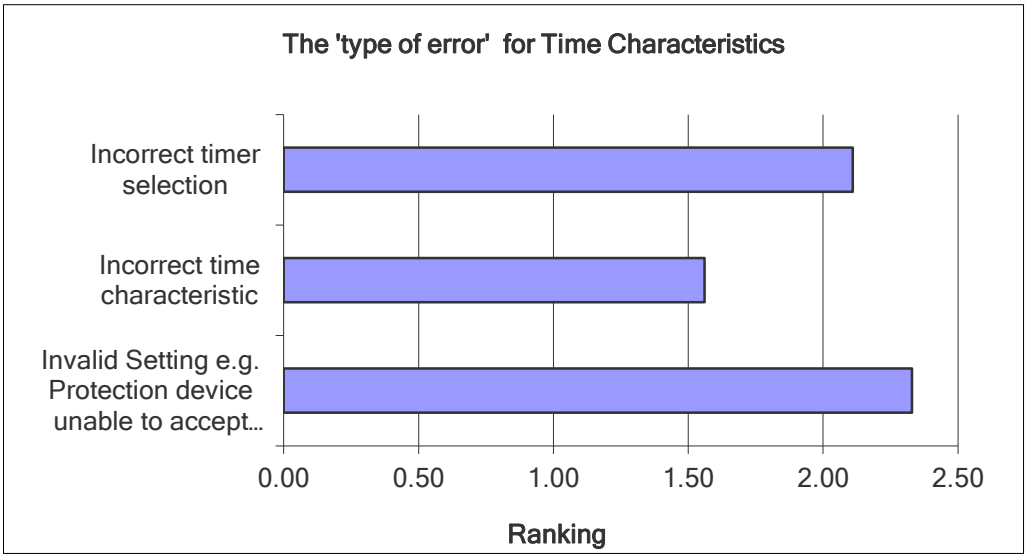


Figure 66: Perception Survey - The 'type of error' for Time Characteristics

C.3.3 Origin and Type of Errors for Control or Indication

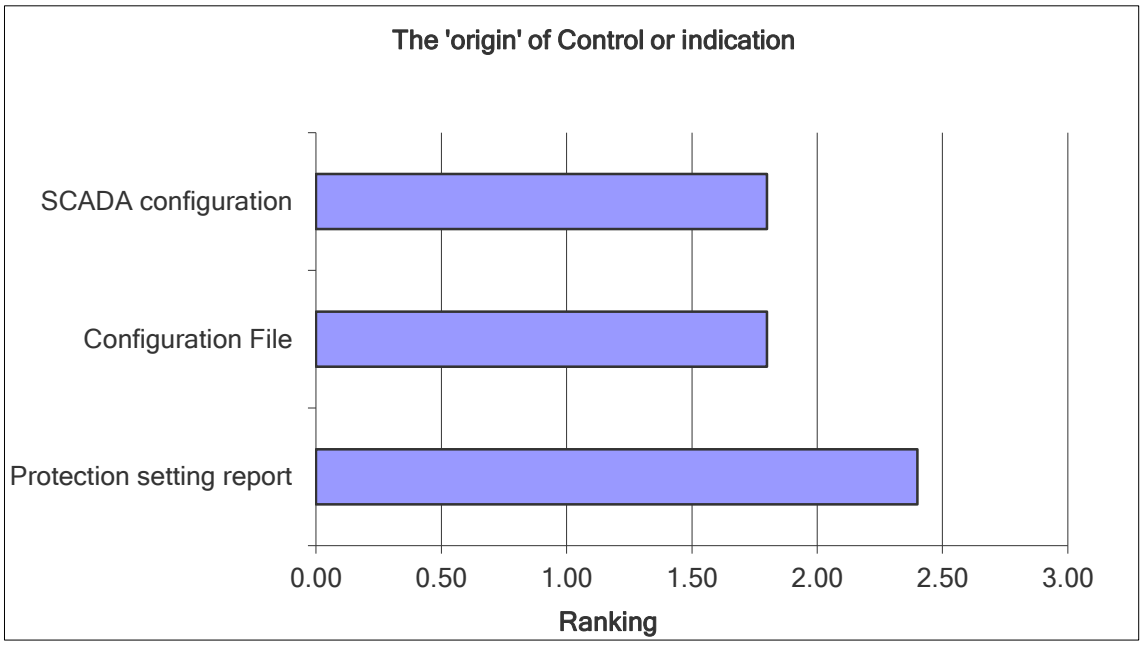


Figure 67: Perception Survey - The 'origin' of Control or Indication errors

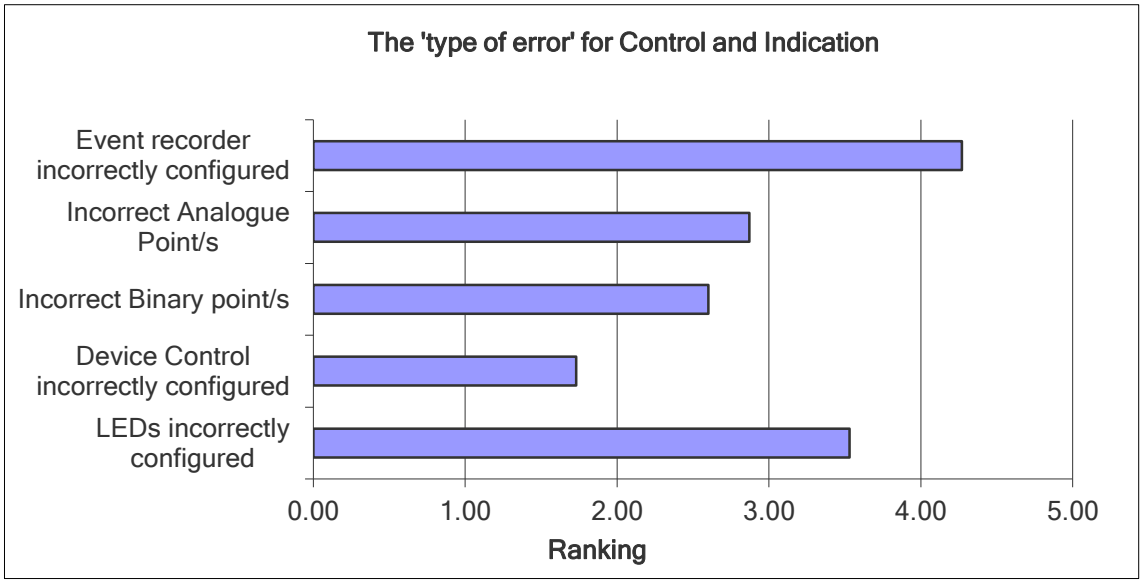


Figure 68: Perception Survey - The 'type of error' for Control or Indication

C.3.4 Origin and Type of Errors for Device Firmware

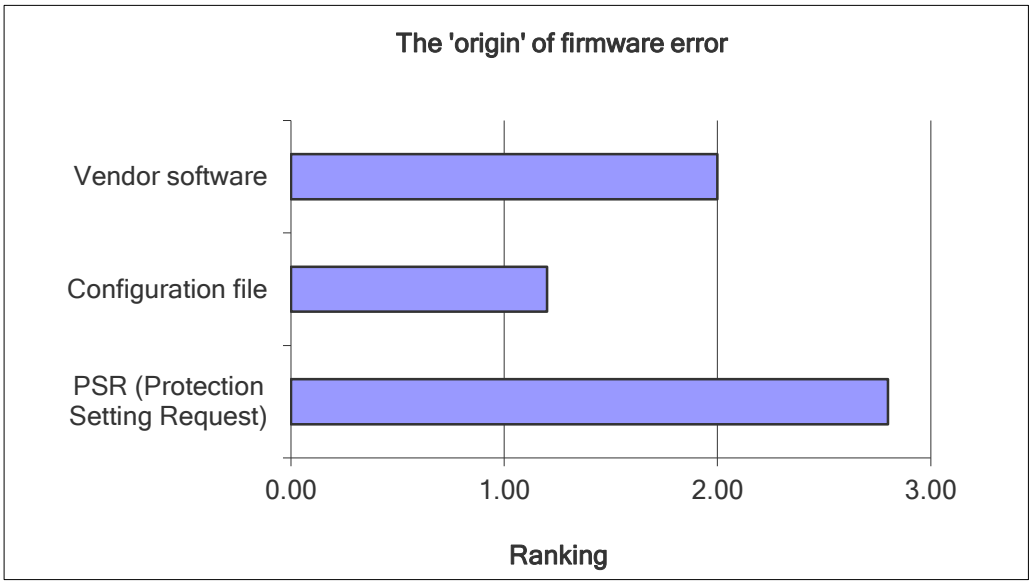


Figure 69: Perception Survey - The 'origin' of Firmware errors

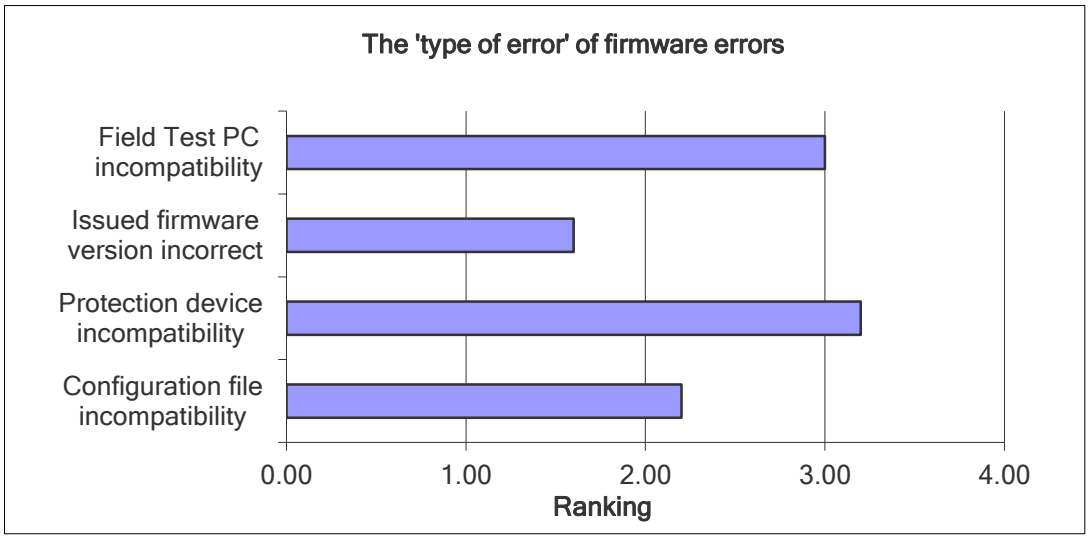


Figure 70: Perception Survey - The 'type of error' for Firmware

Appendix D: SQL code used for Benchmarking

The is the SQL Code developed to enable data mining of Ergon Energy's Protection Database System (PDS) as described in section 3.3.2.

D.1 SQL code for SQL Query 1

```
SELECT PROTMAIN.PROT_PSR.PSR_ID,
PROTMAIN.PROT_PSR.STATUS,
PROTMAIN.PROT_RELAY_VOLTAGE.VOLTAGE,
PROTMAIN.PROT_RELAY_SETTING_SLOT.ITEM_NAME_1,
PROTMAIN.PROT_RELAY_APPLICATION.APPLICATION_DESC,
PROTMAIN.PROT_RELAY_MANUFACTURERS.MANUFACTURER,
PROTMAIN.PROT_RELAY_SETTING.REQUIRED_SETTING,
PROTMAIN.PROT_RELAY_SETTING_GROUP.SETTING_GROUP_NO AS
SETTING_GROUP_NO1,
PROTMAIN.PROT_RELAY_RC_MAP.RC_MAP,
PROTMAIN.PROT_PROTECTION_TYPES.NAME,
PROTMAIN.PROT_RELAY_SUB_TYPE.SUBTYPE,
PROTMAIN.PROT_RELAY_SETTING.SETTING,
PROTMAIN.PROT_RELAY_SETTING_SLOT.SLOT_TYPE,
PROTMAIN.PROT_RELAY_TEMPLATE.RELAY_ID,
PROTMAIN.PROT_RELAY_SETTING_SLOT.ACTIVE,
PROTMAIN.PROT_RELAY_TYPE.RELAY_TYPE_ID
FROM PROTMAIN.PROT_PSR
INNER JOIN PROTMAIN.PROT_RELAY_TEMPLATE
ON PROTMAIN.PROT_RELAY_TEMPLATE.TEMPLATE_ID =
PROTMAIN.PROT_PSR.TEMPLATE_ID
INNER JOIN PROTMAIN.PROT_RELAY_SETTING_SLOT
ON PROTMAIN.PROT_RELAY_SETTING_SLOT.ID =
PROTMAIN.PROT_PSR.SLOT_ID
INNER JOIN PROTMAIN.PROT_RELAY_VOLTAGE
ON PROTMAIN.PROT_RELAY_VOLTAGE.ID =
PROTMAIN.PROT_RELAY_SETTING_SLOT.VOLTAGE_ID
INNER JOIN PROTMAIN.PROT_RELAY_APPLICATION
```

```
ON PROTMAIN.PROT_RELAY_APPLICATION.APPLICATION_ID =
PROTMAIN.PROT_RELAY_TEMPLATE.APPLICATION_ID
INNER JOIN PROTMAIN.PROT_RELAY_ID
ON PROTMAIN.PROT_RELAY_TEMPLATE.RELAY_ID =
PROTMAIN.PROT_RELAY_ID.ID
INNER JOIN PROTMAIN.PROT_RELAY_MANUFACTURERS
ON PROTMAIN.PROT_RELAY_ID.MANUFACTURER_ID =
PROTMAIN.PROT_RELAY_MANUFACTURERS.MANUFACTURER_ID
INNER JOIN PROTMAIN.PROT_RELAY_SETTING
ON PROTMAIN.PROT_PSR.PSR_ID =
PROTMAIN.PROT_RELAY_SETTING.PSR_ID
INNER JOIN PROTMAIN.PROT_RELAY_SETTING_GROUP
ON PROTMAIN.PROT_RELAY_SETTING.SETTING_GROUP_NO =
PROTMAIN.PROT_RELAY_SETTING_GROUP.SETTING_GROUP_ID
INNER JOIN PROTMAIN.PROT_RELAY_RC_MAP
ON PROTMAIN.PROT_RELAY_SETTING.ERGON_NAME_ID =
PROTMAIN.PROT_RELAY_RC_MAP.ERGON_NAME_ID
AND PROTMAIN.PROT_RELAY_SETTING.TYPE_ID     =
PROTMAIN.PROT_RELAY_RC_MAP.TYPE_ID
INNER JOIN PROTMAIN.PROT_RELAY_SUB_TYPE
ON PROTMAIN.PROT_RELAY_SETTING.SUB_TYPE_ID =
PROTMAIN.PROT_RELAY_SUB_TYPE.SUBTYPE_ID
INNER JOIN PROTMAIN.PROT_PROTECTION_TYPES
ON PROTMAIN.PROT_RELAY_SETTING.TYPE_ID =
PROTMAIN.PROT_PROTECTION_TYPES.TYPE_ID
INNER JOIN PROTMAIN.PROT_RELAY_TYPE
ON PROTMAIN.PROT_RELAY_TYPE.RELAY_TYPE_ID =
PROTMAIN.PROT_RELAY_ID.TYPE_ID
WHERE (PROTMAIN.PROT_PSR.STATUS         = 'Approved'
OR PROTMAIN.PROT_PSR.STATUS             = 'Completed'
OR PROTMAIN.PROT_PSR.STATUS             = 'Finalised'
OR PROTMAIN.PROT_PSR.STATUS             = 'Issued')
AND PROTMAIN.PROT_RELAY_VOLTAGE.VOLTAGE   = 11
AND (PROTMAIN.PROT_RELAY_APPLICATION.APPLICATION_DESC LIKE
'%DISTRIBUTION%'
```

```
OR PROTMAIN.PROT_RELAY_APPLICATION.APPLICATION_DESC LIKE
'%RECLOSER%')
AND PROTMAIN.PROT_RELAY_SETTING_GROUP.SETTING_GROUP_NO = 1
AND PROTMAIN.PROT_RELAY_RC_MAP.RC_MAP              = 'OC PICKUP'
AND (PROTMAIN.PROT_RELAY_SUB_TYPE.SUBTYPE           = 'STAGE 1'
OR PROTMAIN.PROT_RELAY_SUB_TYPE.SUBTYPE            = 'IDMT'
OR PROTMAIN.PROT_RELAY_SUB_TYPE.SUBTYPE            = 'OC')
AND PROTMAIN.PROT_RELAY_SETTING_SLOT.SLOT_TYPE      = 'RLFLD'
AND PROTMAIN.PROT_RELAY_SETTING_SLOT.ACTIVE         = 'Y'
AND (PROTMAIN.PROT_RELAY_TYPE.RELAY_TYPE_ID         = 1
OR PROTMAIN.PROT_RELAY_TYPE.RELAY_TYPE_ID           = 4
OR PROTMAIN.PROT_RELAY_TYPE.RELAY_TYPE_ID           = 3
OR PROTMAIN.PROT_RELAY_TYPE.RELAY_TYPE_ID           = 2)
```

To find the outgoing 11kV feeder Earth Fault and Sensitive Earth Fault tripping threshold settings the following code replaced the Overcurrent SQL code within the outline boxes.

```
AND PROTMAIN.PROT_RELAY_RC_MAP.RC_MAP              = 'EF PICKUP'
AND (PROTMAIN.PROT_RELAY_SUB_TYPE.SUBTYPE           = 'STAGE 1'
OR PROTMAIN.PROT_RELAY_SUB_TYPE.SUBTYPE            = 'IDMT'
OR PROTMAIN.PROT_RELAY_SUB_TYPE.SUBTYPE            = 'EF')
```

```
AND PROTMAIN.PROT_RELAY_RC_MAP.RC_MAP              = 'SEF PICKUP'
AND PROTMAIN.PROT_RELAY_SETTING_SLOT.SLOT_TYPE      = 'RLFLD'
```

D.2 SQL code for SQL Query 2

```
SELECT PROTMAIN.PROT_PSR.PSR_ID,
  PROTMAIN.PROT_PSR.STATUS,
  PROTMAIN.PROT_RELAY_VOLTAGE.VOLTAGE,
  PROTMAIN.PROT_RELAY_SETTING_SLOT.ITEM_NAME_1,
  PROTMAIN.PROT_RELAY_APPLICATION.APPLICATION_DESC,
  PROTMAIN.PROT_RELAY_MANUFACTURERS.MANUFACTURER,
  PROTMAIN.PROT_RELAY_SETTING.REQUIRED_SETTING,
  PROTMAIN.PROT_RELAY_SETTING_GROUP.SETTING_GROUP_NO AS
SETTING_GROUP_NO1,
  PROTMAIN.PROT_RELAY_RC_MAP.RC_MAP,
  PROTMAIN.PROT_PROTECTION_TYPES.NAME,
  PROTMAIN.PROT_RELAY_SUB_TYPE.SUBTYPE,
  PROTMAIN.PROT_RELAY_SETTING.SETTING,
  PROTMAIN.PROT_RELAY_SETTING_SLOT.SLOT_TYPE,
  PROTMAIN.PROT_RELAY_TEMPLATE.RELAY_ID,
  PROTMAIN.PROT_RELAY_SETTING_SLOT.ACTIVE
FROM PROTMAIN.PROT_PSR
INNER JOIN PROTMAIN.PROT_RELAY_TEMPLATE
ON PROTMAIN.PROT_RELAY_TEMPLATE.TEMPLATE_ID =
PROTMAIN.PROT_PSR.TEMPLATE_ID
INNER JOIN PROTMAIN.PROT_RELAY_SETTING_SLOT
ON PROTMAIN.PROT_RELAY_SETTING_SLOT.ID =
PROTMAIN.PROT_PSR.SLOT_ID
INNER JOIN PROTMAIN.PROT_RELAY_VOLTAGE
ON PROTMAIN.PROT_RELAY_VOLTAGE.ID =
PROTMAIN.PROT_RELAY_SETTING_SLOT.VOLTAGE_ID
INNER JOIN PROTMAIN.PROT_RELAY_APPLICATION
ON PROTMAIN.PROT_RELAY_APPLICATION.APPLICATION_ID =
PROTMAIN.PROT_RELAY_TEMPLATE.APPLICATION_ID
INNER JOIN PROTMAIN.PROT_RELAY_ID
ON PROTMAIN.PROT_RELAY_TEMPLATE.RELAY_ID =
PROTMAIN.PROT_RELAY_ID.ID
INNER JOIN PROTMAIN.PROT_RELAY_MANUFACTURERS
```

```
ON PROTMAIN.PROT_RELAY_ID.MANUFACTURER_ID =
PROTMAIN.PROT_RELAY_MANUFACTURERS.MANUFACTURER_ID
INNER JOIN PROTMAIN.PROT_RELAY_SETTING
ON PROTMAIN.PROT_PSR.PSR_ID =
PROTMAIN.PROT_RELAY_SETTING.PSR_ID
INNER JOIN PROTMAIN.PROT_RELAY_SETTING_GROUP
ON PROTMAIN.PROT_RELAY_SETTING.SETTING_GROUP_NO =
PROTMAIN.PROT_RELAY_SETTING_GROUP.SETTING_GROUP_ID
INNER JOIN PROTMAIN.PROT_RELAY_RC_MAP
ON PROTMAIN.PROT_RELAY_SETTING.ERGON_NAME_ID =
PROTMAIN.PROT_RELAY_RC_MAP.ERGON_NAME_ID
AND PROTMAIN.PROT_RELAY_SETTING.TYPE_ID     =
PROTMAIN.PROT_RELAY_RC_MAP.TYPE_ID
INNER JOIN PROTMAIN.PROT_RELAY_SUB_TYPE
ON PROTMAIN.PROT_RELAY_SETTING.SUB_TYPE_ID =
PROTMAIN.PROT_RELAY_SUB_TYPE.SUBTYPE_ID
INNER JOIN PROTMAIN.PROT_PROTECTION_TYPES
ON PROTMAIN.PROT_RELAY_SETTING.TYPE_ID  =
PROTMAIN.PROT_PROTECTION_TYPES.TYPE_ID
WHERE (PROTMAIN.PROT_PSR.STATUS       = 'Approved'
OR PROTMAIN.PROT_PSR.STATUS           = 'Completed'
OR PROTMAIN.PROT_PSR.STATUS           = 'Finalised'
OR PROTMAIN.PROT_PSR.STATUS           = 'Issued')
AND PROTMAIN.PROT_RELAY_VOLTAGE.VOLTAGE = 11
AND PROTMAIN.PROT_RELAY_APPLICATION.APPLICATION_DESC LIKE
'%RECLOSER%'
AND PROTMAIN.PROT_RELAY_SETTING_GROUP.SETTING_GROUP_NO = 1
AND PROTMAIN.PROT_RELAY_RC_MAP.RC_MAP               = 'OC PICKUP'
AND PROTMAIN.PROT_RELAY_SETTING_SLOT.SLOT_TYPE      = 'RCFLD'
AND (PROTMAIN.PROT_RELAY_TEMPLATE.RELAY_ID          = 134
OR PROTMAIN.PROT_RELAY_TEMPLATE.RELAY_ID            = 4766
OR PROTMAIN.PROT_RELAY_TEMPLATE.RELAY_ID            = 3444
OR PROTMAIN.PROT_RELAY_TEMPLATE.RELAY_ID            = 4567
OR PROTMAIN.PROT_RELAY_TEMPLATE.RELAY_ID            = 5386)
AND PROTMAIN.PROT_RELAY_SETTING_SLOT.ACTIVE         = 'Y'
```

To find to the downstream 11kV feeder Earth Fault and Sensitive Earth Fault tripping threshold settings the following code replaced the Overcurrent SQL code within the boxed outline.

```
AND PROTMAIN.PROT_RELAY_RC_MAP.RC_MAP                = 'EF PICKUP'
AND PROTMAIN.PROT_RELAY_SETTING_SLOT.SLOT_TYPE       = 'RCFLD'
```

```
AND PROTMAIN.PROT_RELAY_RC_MAP.RC_MAP                = 'SEF PICKUP'
AND PROTMAIN.PROT_RELAY_SETTING_SLOT.SLOT_TYPE       = 'RCFLD'
```

Appendix E: Case Study

E.1 Case Study –Extracted Configuration Discrepancy

This case study highlighted an area of deficiency with the existing configuration management process during verification of a configuration file.

During routine works to extract a configuration file from a manufacturer's 'X' Protection IED a discrepancy was found within the configuration file. The configurable file allocates and publishes push button controls and alarm lamps to the Protection IED's HMI. The reported discrepancy was missing functional logic that is used to identify incorrect phase sequence during recloser commissioning.

In attempt to correct the discrepancy, the missing logic was re-applied to the configuration file and the file was written to the device on the premise that the logic had been inadvertently removed during commissioning testing. Once uploaded to the Protection IED, a comparison between the upload configuration file and extracted configuration file was undertaken. The comparison identified the discrepancy had returned.

To further evaluate the effect of the error, the issued configuration file was uploaded to a test relay and the function in question tested to determine whether it was operating as configured.

The testing found the configured function worked and operated as intended. When the configuration file was extracted from the test relay, saved as the extracted configuration file, and compared with the off line configuration file, the function was again omitted from the extracted file. The extracted file was then rewritten to the protection IED and the function retested to determine whether it was operational; and determined it was again omitted from the Protection IED.

The tests undertaken confirmed when the configuration file containing required feature was written to the Protection IED, the feature was received and would take effect. However when the configuration file is extracted from the Protection IED the function is not published to the extracted file.

This failure not to publish all features to the extracted configuration file questions the suitability of the traditional delivery process to be used to perform emote delivery verification; as the extracted configuration file from the Protection IED does not

represent the configuration that has been upload. The traditional delivery process places importance on the extracted file being identified as the commissioned/ in service configuration.

Under the traditional delivery process the extracted file would need to be corrected external to the Protection IED prior to storing the file into Ergon Energy's PDS. This would involve manual manipulation of the setting file and would introduce the possibility of further human error and would no longer be considered as the in-service, tested configuration file.

E.2 Case Study Outcome

The manufacturer was contacted and believed it was an incompatible firmware issue. The Protection IED's firmware was corrected and the discrepancy was no longer repeatable. The case study highlighted a number of items;

- Steps within the Protection Setting workflow regarding the comparison of configuration files are not being adhered to
- The importance of the approved configuration file
- Re-evaluating the importance of the extracted configuration file.
- An extracted configuration file that is placed into the Protection Database System (PDS) may not be representative of the actual installed configuration.

Appendix F: Comparison Table

F.1 Benefits of the new verification process

Table 18 provides a strength and weakness comparison between the existing delivery and management process and the alternate process described in sections 5.1 and 5.2.

Table 18: Comparison of configuration management processes

Process	Strengths	Weaknesses
Traditional Configuration Management and delivery (Section 5.1)	• The configuration file is independently tested for error with both the hardware and software components of the protection IED tested. • Protection setting changes effectively imposes maintenance action of the protection IED.	• Unable to monitor whether the processes developed to help mitigate possible errors during import process into vendor software is adhered too. • Travel and Site access required • Delays in Configuration delivery
New Configuration Management and delivery (Section 5.2	• Expedited delivery of settings especially for critical operational requirements • Consistent and traceable error reporting can be undertaken • Test staff have immediate access to the Protection setter	• There is an expectation the protection IED to be reconfigured is part of scheduled maintenance program. • Removes opportunity for non-scheduled hardware health verification

Process	Strengths	Weaknesses
	• Expedited response to errors from protection setter owing to a reduce time period between the issuing of configuration to when testing is undertaken • Less travel requirements for staff • Improved learning environment for less experienced test staff	

Appendix G: Risk Assessment

G.1 Personnel safety/Risk Assessments

The risk assessments provided account for the two components relating to the project. The first assessment identifies hazards related to testing of the remote configuration using the remote relay rack. To perform these types of activities it is mandatory that an Ergon Energy Daily Task Risk Assessment Plan (DTRMP) be completed to help determine the risk of personnel injury based on the matrix outlined in Table 19. These daily risk assessments identify the associated hazards and the control measures needed to be implemented to maintain a safe work site. When required assessments will be completed prior to work and will address the activities required.

Table 19: Internal DTRMP "Level of Risk" indicator (Ergon Energy 2013)

Consequence	Likelihood				
	Rare	Unlikely	Possible	Likely	Almost Certain
Catastrophic	Medium	High	High	Extreme	Extreme
Major	Medium	Medium	High	High	Extreme
Moderate	Low	Medium	Medium	High	High
Minor	Very Low	Low	Medium	Medium	Medium
Insignificant	Very Low	Very Low	Low	Medium	Medium

The proposed testing is to be performed in a test laboratory which will involve injection of lethal currents and voltages into a test box that will simulate the primary power system to the basic IED. The electric shock consequence has been rated 'major' owing to the seriousness of receiving a shock however the likelihood of receiving a shock has been classed as 'rare' owing to the leads connected to the relay are fully insulated and work will be performed from a remote location where the test equipment is already installed.

Using the above DTRMP this produces a risk of medium. Although the testing will be in a controlled environment to further control this risk constant communication with an employee located in the test laboratory will be employed during the required tests to ensure all personnel are clear from the area and operation of equipment is as expected.

G.2 Project Risk Assessment

G.2.1 Task Risks

Table 20 outlines those components of the project though theoretical may impact on the time line of the project. These risks have been identified and methods of mitigation have been described.

Table 20: Project risk assessment

Task	Hazard	Initial Risk	Minimisation	New Risk Level
Field Survey 1	Surveys not completed	HIGH	Discussions with field staff supervisors have been undertaken to develop support for the survey to be completed.	MEDIUM
Field Survey 2	Surveys not completed	HIGH	Create email list of field staff and send reminders on fortnightly basis.	MEDIUM
Use of SQL query software	Understand the SQL program and tables available within Ergon Energy's	MEDIUM	Source expert advice within Ergon Energy's Protection group	LOW

Task	Hazard	Initial Risk	Minimisation	New Risk Level
	protection database to extract the required data to provide initial bench marking results			
Bench Marking of Protection settings	Accessing between Ergon Energy's protection database and the Asset management tool to provide a more granule approach for bench marking studies	HIGH	Source expert advice within Ergon Energy's Asset management group	MEDIUM - LOW
Testing of Basic IED responses to setting changes	Access to required protection IED and test equipment	HIGH	Communication with lab test panels already establish and test software and equipment also available	LOW

G.2.2 Project Consequential Effects

The primary focus of this project is the development of processes that can further improve methods of interaction with Ergon Energy's suite of protection IEDs. There is

an expectation from my industry supervisor that the project outcomes from this dissertation, or part thereof, can be implemented within a business strategy for remote configuration management of protection IEDs.

This highlights consequence of the project outcomes to ensure that they are clear and concise with any proposed change in methodology concerning Ergon Energy's safety systems. The project's outcomes will need to include clear technical explanations for proposed changes, clearly state their limitations and those additional requirements needed to support any changes to ensure compliance to all legislative, regulatory and standards of the relevant authorities imposed onto electricity entities.

The risk associated with changing functions of a safety system without maintain appropriate and best practice engineering design and rigour introduces a risk evaluation of the consequence to be 'Catastrophic' and the likelihood of 'Possible/Likely' providing a an overall risk of 'High/Extreme' using the DTRMP in Table 20.

G.3 Risk Likelihood Table

The Risk Likelihood Table is used to assess the likelihood of a risk occurring and in applying it one or more relevant likelihood rating definitions can be used to determine the likelihood rating (Ergon Energy 2013).

Table 21: Risk likelihood table

Likelihood Rating	Likelihood Rating Definitions
Almost Certain	(1) Probability of occurrence – 90% (2) Expected to occur every 12 months (3) The event is expected to occur in most circumstances as there is a history of regular occurrence
Likely	(1) Probability of occurrence – 70% (2) Expected to occur every 1 to 5 years (3) The is strong possibility the event may occur as there is a history of frequent occurrence

Likelihood Rating	Likelihood Rating Definitions
Possible	(1) Probability of occurrence – 50% (2) Expected to occur every 5 to 15 years (3) The event may occur at some time as there is a history of casual occurrence
Unlikely	(1) Probability of occurrence – 30% (2) Expected to occur every 15 to 50 years (3) Not expected to occur, but there is a slight possibility it may occur at some time
Rare	(1) Probability of occurrence – 10% (2) Expected to occur every 50 to 100 years (3) Highly unlikely, but it may occur in exceptional circumstances, but probably never will.

G.4 Risk Consequence Table

The Risk Consequence Table is used to assess the consequence/s or impact/s of a risk and in applying it one or more consequence relevant categories can be used to determine the consequence rating (Ergon Energy 2013).

Table 22: Risk consequence table

Consequence / Impact Category	Consequence / Impact Rating Definitions				
	Catastrophic	Major	Moderate	Minor	Insignificant
Health & Safety	Single fatality of staff, contractor or public	Non-recoverable occupational illness or permanent injury Injury or illness requiring admission to hospital	Injury or illness requiring medical treatment by a doctor	Injury requiring first aid Circumstances that lead to a near miss	Not applicable