University of Strathclyde

Department of Electronic and Electrical Engineering

A RISK ASSESSMENT FRAMEWORK FOR POWER SYSTEM PROTECTION SCHEMES

ADRIANTI

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

Doctor of Philosophy

2015

Signed: Adrianti

Date: 28/05/2015

All the praise is due to Allah

This thesis is dedicated to my beloved parents

Acknowledgments

I would like to express my warmest thank to my supervisor, Dr Adam Dysko, for his support and guidance throughout my study. Your encouragement has made my PhD journey become a more rewarding and enjoyable experience.

I also would like to thank the DGHE Indonesia for supporting my research through the scholarship. My gratitude is also go to my colleague Ibrahim Abdulhadi, who has allowed me to use his simulation model for one of my case study and spent a considerable amount of time to give me feedback and advice. My appreciation is also due to Xue Cao for sharing her experience in power system simulation.

Finally, and most importantly I would like to thanks my husband for his patience and encouragement to keep going with my research and writing. For my daughters, thank you for your understanding that we had less time to spend together.

Abstract

Performance of power system protection is determined by the protection system objectives such as dependability, security, selectivity and speed. However, these objectives often conflict one another where an enhancement of performance with respect to one objective causes a deterioration of another. Therefore, the protection design and setting must provide the optimal level of performance based on carefully considered compromise among the objectives. This thesis proposes that the best compromise can be achieved when the minimum overall risk introduced by a given protection scheme is considered as a decision guiding principle. The risk is calculated as a product of the likelihood of the system failure (resulting from protection not operating as intended) and the anticipated failures cost and it can be used to rank alternative solutions or schemes. Such assessment can assist in a protection selection process, evaluation of existing schemes, or finding optimal settings. In order to facilitate the utilisation of risk assessment for power system protection, this thesis proposes a dedicated framework which can help the assessor to perform the risk assessment and report the result to decision makers in an efficient and systematic manner. The framework consists of risk assessment objectives, terminologies, metrics, knowledge of protection and the protected system, scenarios, data, assumptions, and assessment steps. Three case studies are presented to illustrate different intended uses and modelling levels of risk assessment implementation. The first case study evaluates of the existing distance protection on a transmission line after installation of a quadrature booster transformer. The risk result informs the decision making process relating to whether the protection can be maintained or needs to be changed or modified. In the second case study, setting of ROCOF protection is selected based on risk introduced by the settings, hence the optimum setting is the setting with the least risk. The third case study demonstrates application of protection selection i.e. adaptive versus conventional overcurrent protection for a distribution network with DG. The case studies show that risk assessment has been successful in quantifying the overall protection performance according to the intended use and the framework has provided a useful guidance for the assessment.

Table of Contents

List of Figures

List of Tables

Glossary of Terms

ALARP	As Low As Reasonably Practicable
CB	Circuit Breaker
CCGT	Combined Cycle Gas Turbine
CHP	Combined Heat & Power
CPT	Conditional Probability Table
CT	Current Transformer
CVT	Capacitive Voltage Transformer
DG	Distributed Generation
EHV	Extra High Voltage
FMEA	Failure Mode and Effect Analysis
FT	Fault Tree
GTG	Gas Turbine Generator
HAZOP	Hazard and Operability
HSE	Health and Safety Executive
HV	High Voltage
HVDC	High Voltage Direct Current
IDMT relay	Inverse Definite Minimum Time relay
LF	Loading Factor
LOM	Loss Of Main
MTTF	Main Time To Failure
MTTR	Main Time To Repair
NDZ	Non Detection Zone
P1a	Protection at 1a
P34	Protection 34
P43	Protection 43
PLCC	Power Line Carrier Communication
QB	Quadrature Booster transformer
ROC	Renewable Obligation Certificate
ROCOF	Rate Of Change Of Frequency
RTDS	Real Time Digital power system Simulation
UF	Under Frequency
UKGDS	United Kingdom Generic Distribution System
VOLL	Value Of Load Loss
VT	Voltage Transformer
WTG	Wind Turbine Generator

Chapter 1. Introduction

1.1. Background

Power systems cannot be entirely free from faults, therefore fast disconnection of the faulty components is required in order to minimise power outage and to prevent further damage to electrical equipment. This goal is achieved by installing an appropriate protection scheme that responds to abnormal power system quantity such as current magnitude, impedance or rate of frequency change. The choice of power quantity to be monitored by the protection system depends on the protected system characteristics and the type of abnormal condition to be detected. At low and medium voltage distribution level, current magnitude monitoring is usually sufficient for fault detection and satisfactory protection performance. However, on HV transmission lines, current magnitude cannot provide acceptable discrimination due large variation of current and much shorter operating time requirements. In such cases current phasor or impedance measurement is used. Moreover, for each quantity there are several alternative protection schemes. For example, current magnitude based measurement is adopted by fuse, instantaneous over current relay and Inverse Definite Minimum Time (IDMT) relay with many variants.

Due to high number of available options, the selection of the most appropriate protection method can sometimes be difficult. The existing approaches of protection scheme selection are mainly based on the past practice which takes into account criticality of the protected component, cost of the protection system, and performance requirements regarding dependability, security, selectivity, stability, speed and sensitivity [1]. However, this selection practice is often insufficient as it cannot accurately compare and rank the protection candidates according their overall long term impact on the protected system. In particular, it does not explicitly quantify the risks associated with protection failure (or spurious operation), hence it does not fully facilitate the selection process.

Moreover, development of new technologies in power system gradually changes the nature of the network and brings new requirements for protection schemes. Installation of distributed generation (DG), for instance, results in a situation where distribution networks no longer operate as passive circuits supplying loads only, but become active and can supply power as well as sustain voltage without connection to the main grid. The active circuit, supplying power to the grid, can change power flow direction in the network. In addition, the DGs become new sources of fault current; hence there is a likelihood of increased network fault levels. Conventional distribution protection systems were designed with the assumed current flow from the grid supply point downstream to the low voltage network. Installation of DG changes this situation, hence the current seen by relays can either increase or decrease depending on position of relays, position of the fault and amount of DG. To ensure correct protection operation, the grading between coordinated relays must be re-evaluated. It must take into account maximum and minimum infeed of all distributed generators as well as the grid supply point [2].

Recent push for the implementation of smart grid technologies also has an impact on protection system requirements. Smart grids change the network from simple radial distribution system to meshed and more intelligent system, which aims to provide enhanced functionality, automation and asset optimisation [3, 4]. The protection system must, therefore, be able to properly isolate faults under changing network topology. The traditional time-current grading coordination may change to adaptive protection which provides sufficient flexibility under topological changes.

Some new intelligent protection schemes have been proposed, such as adaptive protection for distribution lines [5, 6], and for transmission lines [7-10]. However, they need to be assessed in order to choose the best scheme according to the primary system conditions. Therefore, it is important to have a comprehensive tool which can properly cope with complexities when evaluating and comparing protection schemes. The existing protection design and selection methods based on past practice are likely to fall short when dealing with new intelligent schemes as there is no prior experience in most cases. This is one of the main barriers limiting the uptake of new technologies in power system protection.

Reliability analysis of power system protection has been known as a method to evaluate protection scheme design [11-13]. The reliability analysis provides failure mode probabilities in terms of reliability and availability of the protection scheme. However, the results are only a measure of the likelihood of protection failure modes without considering their consequences. Some failure modes have more significant effect than others; therefore they need to be treated differently. For example, in conventional reliability analysis equipment which has high probability of failure but small (or negligible) failure consequences would be ranked as less reliable than the equipment which has low failure probability but catastrophic failure consequences. Moreover, the reliability analysis output is expressed in terms of probability figures of each failure mode which is not always meaningful when it comes to decision making.

Risk assessment, on the other hand, evaluates failure probabilities but also takes into account their consequences. The risk assessment result provides a single quantity that can be compared between alternative solutions in a straightforward way. This nature makes risk assessment a good candidate for an additional mechanism which can support the existing protection design and selection practice. Risk assessment is a well-known method which has been adopted widely in many areas such as nuclear power plants, offshore installations, chemicals industry and gas turbine [14, 15] but not commonly used in the assessment of power system protection schemes. Although not extensive, there are a few existing publications related to power system protection risk assessment:

a. Risk assessment of Special Protection System (SPS) to establish the arming point of installation of SPS in the system [16]. Arming point is a condition where the SPS should start to engage with the system. Below the arming point the risk brought by the SPS is higher than its benefit. However in this publication the consequences of the protection failure mode are not fully explored, i.e. only generation start-up and re-dispatch cost are considered. This may produce incorrect arming point of the SPS.
b. Risk assessment which gives quantitative basis as a guideline in the trade-off between sensitivity and security requirement in ground fault protection [17].

The paper is assessing the risk of individual safety due high resistance faults in MV network and the risk result can be used to as standard for ground protection design.

c. Individual safety risk assessment of non-detection zone of ROCOF protection as a guidance to implemented Neutral Voltage Displacement Protection as back up of the ROCOF protection [18]. This assessment only focuses to the individual risk hence all possible consequences are not fully developed. Similar risk assessment is conducted by the same author for different ROCOF protection settings to inform the review of the setting guidelines in UK in anticipation of diminishing inertia in GB power system [19].
d. Distance protection risk assessment is presented in [20] however, the consequences which are considered are only limited to demand loss which does not fully represent the protection failure mode consequences.
e. An on-line distance protection risk assessment for monitoring purposes is presented in [21]. The values of failure consequences are quantified in terms of indices of violation of voltage magnitude, active and reactive power and demand loss. The total risk is calculated from the indices multiplied by their weighting factors. However, the paper fails to provide the methodology to quantify the weighting factors which are the important part of the assessment.

In conclusion, there are various limitations of these publications such as:

- Assessment only for one of the failure modes.
- Consequences of the protection failure modes are not fully explored.
- Value of the consequences is not expressed in the most appropriate way.

Therefore, there is a need to develop a comprehensive risk assessment framework which can be used as an important element in establishing the best protection practice for a given protected system.

1.2. Research question

The key research questions posed at the outset of this thesis are as follows:

a. What is the best way (or criteria) to choose a protection scheme for a given power system?
b. Does the risk assessment provide additional value in the selection of protection schemes, evaluation of existing protection or in the process of establishing the optimal settings?
c. If so, how to perform protection risk assessment in an efficient and systematic manner?

The research work presented in this thesis aims to provide a reasoned response to these questions.

1.3. Summary of key contributions

In order to address the research questions outlined in the previous section the thesis has made a number of contributions which can be summarised as follows:

a. Through systematic study, risk assessment has been identified as a very convenient and comprehensive method to rank protection candidates according to their overall performance, and thus, can complement the existing protection selection process. Risk assessment quantifies the risk of utilising given protection candidates based on their failure mode likelihood combined with failure consequences.
b. A dedicated framework for risk assessment of power system protection schemes has been proposed and developed. This framework is intended to form a part of the protection decision making process as it will guide the risk assessors in conducting and reporting the assessment in a systematic and transparent manner which can be understood by the decision makers.
c. A systematic methodology to quantify the consequences of protection failure modes has been designed, including the cost of generation and demand disconnection, equipment damage cost, and individual safety.
d. An algorithm for assessing the need to modify the existing protection schemes under changing primary system configurations has been developed. It starts from assessing the risk of maintaining current protection architecture, followed by

establishing the best scheme from the available alternatives, and finally finding optimum protection settings.

e. It has been demonstrated using case studies that the proposed risk assessment can be successfully applied in choosing the most suitable protection scheme, establishing optimal protection settings, as well as assessing the risk of existing schemes under changing system conditions.

1.4. Thesis outline

The thesis is organised as follows:

Chapter 2 introduces power system protection. It describes power system protection objectives, dependability and security, components, types and existing protection scheme selection practices, as well as challenges in designing future protection schemes. It also highlights the limitations of the existing protection practices when faced with the integration of new power system technologies. Systematic and transparent risk assessment approach is identified as a missing element in those practices.

Chapter 3 describes general risk assessment methodology which consists of its definition, steps involved in conducting risk assessment, data and its application. Several well-known probability calculation techniques are also explained and compared. This chapter reveals a need of a dedicated power system protection risk assessment framework.

Chapter 4 explains the proposed risk assessment framework for power system protection. The framework is includes the reason, intended use and scope of the assessment, terminology and metrics, knowledge about the protection and the protected power system, scenarios, data and assumptions, and risk assessment steps.

Chapter 5 presents first case study of protection scheme risk assessment, i.e. risk assessment of distance protection after installation of quadrature booster transformer in the transmission line. The aim is to evaluate the performance of the distance protection under influence of the quadrature booster transformer. The risk result informs the decision making process whether to maintain the existing distance protection or change/modify it.

Chapter 6 is second case study i.e. risk assessment application for finding optimum setting of ROCOF protection. The case study addresses the existing serious issue faced by GB power system. It is anticipated that in the future the rate of change of frequency experienced in GB power system will increase due to the continuing reduction of system inertia. This is a consequence of installation of non-synchronous generation and increasing maximum generation loss (n-1 contingency). To anticipate this condition National Grid plans to increase ROCOF protection setting. This thesis proposes risk assessment as a tool to find the optimum setting to achieve a proper trade-off between sensitivity and stability of ROCOF protection. The optimum setting selection is based on the minimum overall risk.

Chapter 7 presents the third case study: risk assessment of adaptive overcurrent protection in distribution network with DGs. The adaptive protection is a candidate protection scheme to be applied on 20kV the distribution network with several DGs. The adaptive protection is assessed to find out whether it provides good performance in terms of risk. The result is compared with the risk of conventional overcurrent protection to provide a systematic risk based argument for or against installation of the adaptive overcurrent protection.

Finally chapter 8 concludes the thesis and highlights potential future avenues of this research.

1.5. Publications

The following publications directly resulted from the research presented in this thesis:

- Adrianti, A. Dysko, "Risk assessment analysis to find optimum ROCOF protection settings", 12th IET International Conference on Developments in Power Systems Protection (DPSP), Copenhagen, 2014, ISBN: 978-1-84919-834-9.

- Adrianti, A, Dysko, “Bayesian Networks for Risk Assessment of New Power System Protection”, poster, presented in Risk and Reliability Modelling of Energy System, in Durham, 27 November 2012
- Adrianti, I. Abdulhadi, A. Dysko, G. Burt, “Assessing the Reliability of Adaptive Power System Protection Schemes”, 11th IET International Conference on Developments in Power Systems Protection (DPSP), Birmingham, 2012, ISBN: 978-1-84919-620-8.
- Adrianti, A. Dysko, G. Burt, “Probability Estimation of the Occurrence of Protection System Failures in Highly Distributed Generation Systems”, 46th International University Power Engineering Conference (UPEC), Soest, Germany, 2011, ISBN: 978-3-8007-3402-3.
- Adrianti, A. Dysko, G Burt, “Risk Assessment of Adaptive Power System Protection Schemes”, Has been submitted to International Transaction on Electrical Energy System, a Wiley Journal Paper (under review)
- Adrianti, A. Dysko, “A Risk Assessment Framework for Power System Protection”, under preparation, to be submitted to an IET journal.

1.6. References for chapter 1

[1] IEEE, "IEEE Guide for Protective Relay Applications to Transmission Lines," vol. IEEE Std C37.113-1999, ed. New York: IEEE, 1999, p. 107.

[2] N. Jenkins, R. Allan, P. Crossley, D. Kirschen, and G. Strbac, *Embedded Generation* vol. 31. London: The Institution of Engineering and Technology, 2008.

[3] R. E. Brown, "Impact of Smart Grid on Distribution System Design " presented at the IEEE Power and Energy Society General Meeting, 2008.

[4] P. P. Varaiya, F. F. Wu, and J. W. Bialek, "Smart Operation of Smart Grid: Risk-Limiting Dispatch," *Proceedings of The IEEE,* vol. 99 january 2011 2011.

[5] S. K. Salman and S. F. Tan, "Adaptive single phase fault identification and selection technique for maintaining continued operaton of distributed generation," presented at the IET International Conference on Developments in Power System Protection, Manchester, 2010.

[6] P. Mahat, Z. Chen, B. Bak-Jensen, and C. L. Bak, "Simple Adaptive Overcurrent Protection of Distribution System with Distributed Generation," *IEEE Transaction on Smart Grid*, vol. early access, 2011.

[7] A. A. Girgis, A. A. Sallam, and A. K. El-Din, "An Adaptive Protection Scheme for Advanced Series Compensated (ASC) Transmission Lines," *IEEE Transaction on Power Delivery*, vol. 13, April 1998 1998.

[8] S. Dambhare, S. A. Soman, and M. C. Chandorkar, "Adaptive Current Differential Protection Schemes for Transmission-Line Protection," *IEEE Transaction on Power Delivery*, vol. 24, October 2009 2009.

[9] A. G. Jongepier and L. v. d. Sluis, "Adaptive Distance Protection of Double-Circuit Lines Using Artificial Neural Networks " *IEEE Transaction on Power Delivery*, vol. 12, 1997.

[10] F. Kawano, G. P. Baber, P. G. Beaumont, K. Fukushima, T. Miyoshi, T. Shono*, et al.*, "Intelligent Protection Relay System for Smart Grid," presented at the Developments in Power System Protection (DPSP 2010), 2010.

[11] P. Anderson, *Power System Protection* New York: IEEE Press, 1999.

[12] P. M. Anderson and S. K. Agarwal, "An improved model for protective-system reliability," *Reliability, IEEE Transactions on,* vol. 41, pp. 422-426, 1992.

[13] A. Hossein Etemadi and M. Fotuhi-Firuzabad, "New Considerations in Modern Protection System Quantitative Reliability Assessment," *Power Delivery, IEEE Transactions on,* vol. 25, pp. 2213-2222, 2010.

[14] J. D. Andrews and T. R. Moss, *Reliability and Risk Assessment*, second ed. London: Professional Engineering Publishing, 2002.

[15] R. R. Fullwood, *Probabilistic safety assessment in the chemical and nuclear industries*, 2 ed. Woburn: Butterworth-Heinemann, 2000.

[16] W. Fu, S. Zhao, J. D. McCalley, V. Vittal, and N. Abi-Samra, "Risk Assessment for Special Protection Systems," *IEEE Transaction on Power Systems*, vol. 17, pp. 63-72, Feb. 2002.

[17] J. L. P. d. Sa and M. Louro, "On Human Life Risk-Assessment and Sensitive Ground Fault Protection in MV Distribution Networks," *IEEE Transaction on Power Delivery*, vol. 25, October 2010 2010.

[18] DCRP-G59-Working-Group, "Embedded generation interface protection: Assessment of risks arising from relaxation in the application of neutral voltage displacement (NVD) interface protection," December 2009.

[19] A. Dysko, I. Abdulhadi, X. Li, and C. Booth, "Assessment of Risk Resulting from the Adjustment of ROCOF Based Loss of Mains Protection Settings, Phase I " University of Strathclyde, Glasgow, 2013. available at : http://www2.nationalgrid.com/UK/Industry-information/Electricity-codes/Grid-code/Modifications/GC0035-GC0079/

[20] D. Zhihui, W. Zengping, and J. Yanjun, "A probabilistic risk assessment method of transmission line distance protection," in *Power and Energy Society General Meeting, 2012 IEEE*, 2012, pp. 1-7.

[21]. Dai, Z. and X. Liu, A new risk assessment method of power system distance protection. International Transactions on Electrical Energy Systems, 2015.

Chapter 2. Power System Protection Design

This chapter is intended to introduce the general concept of power system protection, its main components and some common types of relays. The existing protection selection practices and their drawbacks are also illustrated. Then the challenges brought by future power system technologies to the protection system are introduced. It highlights the need for additional approach to the existing protection scheme selection. Risk assessment is proposed to mitigate the draw-backs of the current protection scheme selection practices in order to meet power system protection requirements in the future.

2.1. Power system protection objective

Power system protection is one of the most important components of an electrical power system in order to ensure safe operation of a power system. A power system cannot completely avoid the occurrence of faults even for a well-designed power system. A fault can damage the equipment and endanger people if it is not disconnected from the rest of the system immediately. A power system protection detects and disconnects a fault section in milliseconds therefore avoid any damage. This also maintains power system operation for rest of the system.

There are many types of protection system to protect different parts of a power system. However in general, a protection system must have four main principles: sensitivity, selectivity, speed and stability [1-3] as explained in next section.

2.1.1. Sensitivity

Sensitivity is related to the lowest fault quantities that can cause protection to operate. A sensitive protection can detect a fault, even for low fault quantity. This ensures that protection will operate for any faults in its protected zone. Modern digital relays and numerical relays have better sensitivity than their predecessor, electromechanical relays. However, some power system condition such as high resistance faults for overcurrent and distance protection and high source-to-line impedance ratios (SIR) for distance protection reduce the capability of the relays to detect the fault and the problem cannot be eliminated by utilising the digital/numerical relays.

2.1.2. Selectivity

Selectivity is the capability of the protection to minimize the protected system outage due to fault clearances. When the fault occurs, the protection should trip the nearest circuit breakers to the fault location and prevent other protection systems from operating, therefore only a limited section of the primary system is disconnected. Therefore selectivity is related to protection coordination where primary protection operates as fast as possible while back-up protection operates after a delay time if the primary protection fails to clear the fault. Good selectivity will maximize the continuity of the services.

2.1.3. Speed

In order to avoid power system damages and instability, a protection system must operate as quickly as possible to isolate the faulted section. The disturbance must be removed before it causes widespread loss of synchronism and it may lead to power system blackout. However if the speed is too fast, the relay become less selective hence cause unwanted operation.

2.1.4. Stability

Stability is ability of a protection to remain stable and not operate for any non-faulted condition and for faults that are the external to its protected zone.

2.2. Protection dependability and security, their effect to power system

Dependability and security are the two aspects of protection reliability. Dependability is a measure of the protection ability to operate for all faults in its protected element. Dependability can be improved by increasing sensitivity of the protection. Security of a protection is ability to prevent protection operation for no fault condition with in its protected element. In other words, security is the ability to prevent unwanted operation. Dependability and security are contrary each other. Increasing protection sensitivity in order to increase its dependability often leads to a reduction in the level of security.

Dependability can be improved by providing redundancy of the protection components, local and remote protection back up, different design of redundancy protection, etc. Security can be improved by applying series connection of the protection, enhancing self-monitoring and supervision and good quality of the components. Series connection is provided by two or more protections which have different operating principles and the circuit breaker only trips if all protection devices send trip commands.

2.3. Power system protection components

In general, protection system equipment consists of three main functions and additional components:

a. Protected (primary) system measurement

   This equipment is usually current and (or) voltage transformer which act as senses of the protection system in order to get the information about the primary system condition. The both equipment are also known as instrument transformers

b. Protection relays

   A protection relay is a brain of a protection system. It decides to operate or not to operate the protection system based on measurement from the transformer(s).

c. Circuit Breaker

   If a protection relay decides to operate (trip), a trip command will be send to a tripping coil of circuit breaker. Then the trip circuit get energized and the circuit breaker opens its contact. Opening circuit breaker contacts cause the disconnection of the faulted parts of the power system.

d. Additional components including DC supply, communication, wiring and self-monitoring/supervision

Details about the protection components are explained in the next section.

2.3.1. Primary system measurement

Current and voltage transformers scale primary system currents and voltages down to a standard value of protective relay i.e. 1 A, 5A and 110V. The reason for reducing the current and voltage is to isolate the protective equipment from high voltage of power system and for safety of operating personnel. The transformer is expected to provide accurate measurement during normal to transient disturbances of the power system hence ensure the protection works correctly.

Current transformer (CT) design has separate primary and secondary winding with the primary winding consist of a single turn known as bar-primary. Unlike CT for measurement purpose, a protective CT is designed to have operating point much below the knee point of excitation characteristic, hence it will not saturate easily during high fault current. To achieve this condition, the CT's cores must have sufficiently large cross-sectional area which also means a more expensive CT. However as the protection needs to work in first few cycles after a fault, the CT can still produce reasonable output before it saturates. For that reason, a smaller core CT sometimes is used to lower the expense [2]. However, the saturation problem may trigger protection unwanted operation of differential protection for fault beyond its protected zone.

A voltage transformer (VT) is connected in shunt to the power system. There are two types of VTs:

- Conventional two winding transformer
- Capacitive voltage transformer (CVT)

CVT is a more economic VT for high voltage as it reduces the size of VT. A capacitor in CVT acts as a potential divider and a series reactor is used to compensate the capacitor during normal frequency. Reactance of the capacitor is cancelled by the reactor reactance therefore the CVT behave like a conventional VT.

There are two types of failures that the protection transformer may suffer i.e. major and minor failures. The major failures inhibit the fundamental function of an instrument transformer to provide current/voltage measurement to a relay. The causes of major failures are including: internal dielectric failures (flash over, partial discharge, breakdown), external dielectric failures (flashover), loss of electrical connection integrity in primary or secondary, leakage of insulation medium, mechanical damage of parts like insulator, providing false signal, accuracy out of tolerances, functional loss of damping circuit and monitoring device failures (oil pressure, SF6 density or free gas detection system). Internal dielectric failures provide the greatest contribution (42.8%) to the failure mode [4]. The minor failures do not prevent the instrument transformer from providing its fundamental function. The causes of minor failures include: changes in dielectric functional characteristics, weakness in electrical connection integrity, leakage in insulation medium, weakness in mechanical integrity, changed characteristics of damping circuit, etc. [4]. Major failure frequencies of instrument transformer (CT and VT) are shown in table 2.1. [4].

Table 2.1. Major failure frequencies of instrument transformers [4]

Voltage Class	Failure frequency (failure/year)
$60 \leq V < 100$ kV	0.000059
$100 \leq V < 200$ kV	0.000655
$200 \leq V < 300$ kV	0.001071
$300 \leq V < 500$ kV	0.000902
$500 \leq V < 700$ kV	0.000084
≥ 700 kV	0.001592
Overall	0.000533

2.3.2. Protection relays

Protection relay technologies have experienced vast developments in the last decade or so. The first technology of protection relay is electromechanical relay which dates back to one hundred years ago. In the early 1960's static relays was introduced, followed by digital relays in 1980 and numerical relays around 1985 [3]. Static and digital relays have been superseded by numerical relays, but electromechanical relays application is still significant until their end life and then being replaced by modern relays.

The electromechanical relays work on principle of generating magnetic force from current flowing in windings of a magnetic core. The magnetic force causes relay contacts to move, hence producing an “on-off” switching operation. The electromechanical relays are highly reliable and robust [5] but each device only performs one relay function.

Static relays use analogue electronic devices to reproduce relay characteristics. These relays provide lower burden for CT/VT and smaller size but it is still in one relay function per case. The main drawback of this relay technology is its sensitivity to electromagnetic interference and the need for very reliable dc power.

Digital relays use microprocessor and microcontroller to implement relay function and introduce analogue to digital conversion for all measured analogue quantities. The microprocessors for digital relays have limited processing capacity and memory compared with numerical relays.

Numerical relays employ powerful microprocessors known as digital signal processor (DSP), along with software to carry out the protection functions. A single unit numerical relay can replace several previously separate protection units hence it will reduce space requirement. Numerical relays also have several additional capabilities to boost the relay performances such as: self-supervision, CT/VT supervision, CB control/condition monitoring, several setting group, disturbance recording, built-in remote communication and built-in back-up. As a single unit, a relay can provide several protective functions; hence there is a concern about the reliability of the protection. A failure of this relay unit can cause loss of many protection functions. But with more advanced technology and good design, numerical relay application experiences show that a multifunction numerical relay is at least as reliable as its predecessor [3].

The self-supervision in a numerical relay will trigger a watchdog alarm if the relay suffers from a failure, hence the operator will know that the relay has failed. The failure rate of a modern numerical relay is 0.018 failure/year and lifetime is predicted around 15 years based on the life of its components i.e. conductor and ICs (Integrated Circuits) [6].

2.3.3. Circuit breaker

Circuit breakers carry out switching operation to disconnect the faulted part(s) of the power system during a fault. When circuit breaker contacts open for switching operation, arcing and restriking voltage occur alternately for the first two or three cycles of power frequency until the contact gaps successfully withstand the restriking voltage. The arc needs to be extinguished soon to prevent its energy melts down the breaker contacts and also to make sure that the faulted section is disconnected quickly. The arc interruption capability depends on dielectric strength and the pressure of insulating medium where the breaker contact is placed. The higher the dielectric strength the faster the arc disappears. Media such as oil, SF6 and vacuum has been used instead of air to provide higher breakdown strength for very high voltage power systems. Failure rates of SF6 circuit breakers based on their nominal voltage is shown in table 2.2.

Table 2.2. Failure rate of SF6 circuit breaker (failure/year) [4]

Rated Voltage Class (KV)	Point estimation	Lower limit	Upper limit
$60 \le V \le 100$	0.0013	0.0011	0.0015
$100 \le V \le 200$	0.0027	0.0024	0.0030
$200 \le V \le 300$	0.0035	0.0030	0.0041
$300 \le V \le 500$	0.0077	0.0067	0.0087
$500 \le V \le 700$	0.0046	0.0030	0.0067
≥ 700	0.0026	0.0041	0.0294
Total	0.0030	0.0028	0.0032

2.3.4. DC supply

DC supplies are required for relays, communication equipment and circuit breakers. Failures of the DC supply results in the protection components failing to operate. Separate DC supplies are normally provided for each relay, circuit breaker and communication equipment. DC supplies consist of batteries and associated charging units. Battery and charging unit failure rate and mean time to repair are shown in table 2.3.

Table 2.3. Failure rate and mean time to repair of a battery and its charging unit [7]

Charger and battery	
Failure rate	0.00741 failures/years
Mean Time to Repair	0.5 hour

2.3.5. Communication

Some types of protection system which use numerical relays need to communicate with remote relays or circuit breakers. The communication message may be in the form of inter tripping (such as tripping/blocking signal in distance protection) or signalling (measurement data, such as in unit protection). Common communication links for protection system are [3]:

- Private pilot wire and channel
- Rented pilot wire and channel from communication company
- Power line carrier communication (PLCC)
- Radio channel
- Fibre optic communication

Pilot wire is the oldest and the most widely used form of protection communication. It consists of a continuous copper link between signalling point. For longer distance, a channel wire which has discontinuous copper link is used. Along the route, it has repeater to boost the signal level and isolation transformers to protect from the rising of ground potential due to earth fault. The wire is sensitive to electrical interference from power circuit or lightning therefore it is only attractive for short distance.

Rented pilot wires eliminate the cost for installation and maintenance but the signal path maybe changed by the pilot wire owner without warning. The wire also has smaller induced voltage from power line as its route is different from the associated power line, although it still suffer from interference of other communication network.

PLCC employ high frequency signal transmission along overhead power line. This communication is more reliable than pilot wires and it is often applied for long distance communication. High noise may come from lightning and system fault inception or clearance, but it lasting in a few milliseconds.

Radio channel is well suited to transmitted bulk of information between major stations, but radio channel has lower reliability than PLCC. Although radio channels are not affected by power system faults but radio equipment itself can produce noises and polluted atmosphere can cause interference.

Optical fibre channels can send huge information and do not have problem with electrical interferences. Information to be transmitted is modulated in form of beam of lights then travel along the fibre. At the receiving end they will decoded into information signals. Optical fibre can transmit hundreds of megahertz data in tens kilometres, for longer distance repeater is needed. In addition for dedicated protection communication, fibre optic channel can also be used to carry all types of communication such as voice and tele-control. It provides very reliable communication.

2.3.6. Self-monitoring/supervision

Numerical protection normally has self-monitoring/supervision for the CT, VT and circuit breaker. The self-monitoring/supervision provides information about failures of the CT, VT or circuit breaker condition hence repair work can be carried out immediately and prevents failure to operate of the protection when a fault occurs. If VT supervision detects no voltage output of a failed VT, it will inform to the relay thus it prevents unwanted operation of the distance relay.

2.4. Types of protection relays

There are many types of existing protection relays with difference principles of operation. Some operation principles of the relays may suitable to detect fault quantity of a protected element hence they are chosen as protection candidates. However economic importance of the protected element versus cost of the protection system will limit the application of some protection. Based on this reason, it is found that similar protected elements of power systems usually have the same protection system. Some well-known relays with their operating principles and application are described in the following section.

2.4.1. Overcurrent relays

An overcurrent relay operates when it senses higher current magnitude than the setting. There are many variants of overcurrent relays according to their discrimination methods such as invers definite minimum time (IDMT), instantaneous and independent definite time. Application of overcurrent relays is including fault and overload protection for equipment in medium voltages, phase and ground fault protection for both induction and synchronous motors, back-up protection for generators, motors or transformers and primary protection for small transformers.

2.4.2. Distance relays

A distance relay observes current and voltage of the line in order to quantify the impedance or admittance of the line and operate if the value less than the setting. Distance relays are applied for primary and back-up protections of transmission lines and back-up protections for large generators.

2.4.3. Differential relays

Differential relays work based on measured currents that entering and leaving the protected zones. If the amount of two currents is not the same then the relay will operate. Differential relays are applied for generators, transformers, and sometime for important transmission lines as the relays will need expensive communication systems.

2.4.4. Frequency relays

Frequency relays operate due to power system frequency that is higher than setting (for over-frequency protection) or lower than setting (for under-frequency protection). This relay is usually applied for generators to avoid prolonged under or over-frequency condition.

2.4.5. Rate Of Change Of Frequency (ROCOF) relays

ROCOF relays work if the rate of system frequency change is higher than the relay setting. The rate of frequency change is calculated every several cycles and the relay will trip if the changing rates remain higher than setting after several measurements. ROCOF relays are employed for Distributed generation (DG) plants to disconnect the DGs following loss of main events hence the DGs are prevented from supplying the islanding network.

2.5. Existing power system protection scheme selection practice

Power system protection failures contribute to 75% of major power system disturbance according a study of NERC (North America Electric Reliability Council) [8]. These protection failures are related to both failure to operate or unwanted operation modes. Moreover, Norwegian fault statistics shows that protection failures become a significant contributor to amount of energy not supplied (ENS) [9] with unwanted operation mode dominated the cause. These data show that correct operation of a protection scheme is a very important aspect for a reliable power system and unwanted operation cannot be considered less important than failure to operate as traditional thought [10].

As performances of the protection system have important consequences to the continuity of power system services, selection of protection schemes to be applied to the system must be carried out carefully. The current practices of power system protection selection are described as follows.

The power system protection scheme selection process is initiated during the design stage of the protected system. The protection criteria must meet the utility requirement of providing [11]:

- Maximum protection for the varying system operating conditions
- Minimum equipment cost
- Reliable
- High speed

- Simple design
- High sensitivity
- Stable for non-fault condition
- Isolate minimum portion of the protected system

However, these criteria are often in conflict with one another. There is no standard way to achieve a compromise of the conflicting criteria. Therefore the judgments in the selection process are often considered an art than a science, according to reference [11].

According to the IEEE standard C37.113-1999, the existing protection selection technique is influenced by several factors i.e.: reliability, sensitivity, selectivity, speed, criticality of the protected element, power system requirement, past practice, communication facility, old or new technology, flexibility, providing redundancy, and design compromise. These factors are explaining as follows.

2.5.1. Reliability, sensitivity, selectivity and speed of the protection

The protection reliability is a level of dependability and security of the protection. The protection should operate when it is supposed to (dependability) and should not operate for other condition (security). The reliability level is measured from a protection reliability test for different system condition.

Good sensitivity ensures dependability of the protection; however a more sensitive protection can cause lowered security. The high speed protection reduces the risk of equipment damages and instability but it may reduce protection selectivity and security. Therefore, a compromise among reliability, sensitivity, selectivity and speed is a problematic task.

2.5.2. Criticality of the protected element

The criticality of the protected element to the power system determines the required reliability level of protection because reliability level of the protection is related to the cost. The criticality of the protected line for example, is based on voltage level, length of the line, closeness to generators, load flow, stability studies, costumer concerns, etc.

2.5.3. Power system condition or requirement

Influence of power system conditions in the protection selection is including:

- ✓ Fault clearing time. In transmission protection for example, fault clearing time affects stability of the system.
- ✓ Fault current level. If the fault current level has significant variation then the protection need flexibility or adaptive functionality.
- ✓ Line configuration such as number of terminal, tapped load/generator, shunt or series inductance/capacitance, requires special consideration.

2.5.4. Communication

Some protection systems operate using communications as an integral scheme element. However the choice of communication based protection may be influenced by two factors:

- ✓ Compatibility with existing power system communication.
- ✓ Characteristics of the communication schemes which are required by the protection.

2.5.5. Past Practice

The past protection type influences the selection of the new protection. Because choosing a completely new type of protection requires more effort to train the responsible personnel and different documentation.

2.5.6. Old versus new technology

Applying old proven technologies provide trustworthy capability. However, applying a new technology, although more risky, it provides interesting features that are not provided by the old technologies, such as better sensitivities, wider setting ranges, greater flexibility, lower burden and reduce panel wiring and panel space.

2.5.7. The future

The protection selection needs to consider the future development in the power system. Therefore the protection design must have flexibility, be easy to modify or even easy to replace.

2.5.8. Redundancy

Failures of protection components can cause protection failures. To prevent protection failures, important protection components usually have backup. The redundancy is also provided for the protection system in terms of local and remote backup.

Failures can also come from common failure modes i.e. a single source of failure that affects more than one protection components. Examples of sources of common failure modes are a type of power system transient condition, incorrect maintenance or calibration procedures. To prevent common failure modes the main and backup protection required to have independence of design i.e. different operating principles and different manufacturers. Also the protection requires varying maintenance personnel from time to time and independent check of settings.

2.5.9. Protective design compromise

To achieve the best protection scheme, some compromises are needed to accommodate the protection conflicted objectives. The compromises are including dependability versus security, reliability versus cost, speed versus security, simplicity versus versatile functionality, independence of design versus standardization and old technology versus new technology. The compromises are carried out based on the knowledge of the most probable failure, recommendation of the equipment supplier, good practical judgment [12].

2.6. Limitation of the existing protection selection practice

The considered factors in protection selection, as mentioned in section 2.5.1. to 2.5.9. are translated to power system protection requirements/policy by power system operators. The requirements are defined for each of protected system, such as transmission line protection, distribution line, substation, generator and transformer according to the voltage level and (or) the capacity. Examples of these protection requirements/policies can be found in reference [13-15] which are Icelandic protection requirement, UK National Grid transmission protection policy and SP power system protection policy respectively. These documents do not describe explicitly how the policies are generated. Moreover, the policies only consider the conventional protection and protected systems; therefore it cannot necessarily deal with future power system technology.

The current practices of power system selection requirements do not have a standard approach to make an optimum compromise between the conflicted objectives of the protection. Traditionally, dependability is often preferred over security especially during non-stressed system [10]. However for a stressed system i.e. a condition when the available reserve generation or transmission capacity in the system is very limited to anticipate a serious contingency, security is considered as important as dependability [16]. Therefore an additional approach is needed to address this issue. The approach should facilitate decision making process when for example in selecting between protection A or B, where protection A has higher level of dependability than protection B, but protection A has a lower level dependability than protection B. The approach should also assist in protection selection process by ranking the protection candidates based on their overall performance.

2.7. Challenge in future power system protection

Introduction of new technologies such as smart grid, distributed generation, storage and HVDC into power systems has brought new protection requirements as the existing conventional protection may fail to provide the protection functionality [17]. The new protection schemes will be in the form of smart protection which need high speed communication, synchronized phasor measurements and wide area measurement [17, 18].

Moreover, since the existing protection schemes are relatively simple hence the deterministic selection technique may be sufficient. However, future protection scheme tends to be more complex with increasing the stochastic nature of power system components such as renewable generation and smart grids [19]. Nowadays, amounts of predicted demand and hence the generator output can usually be predicted with good levels of accuracy using historical data and forecasting models, although they are probabilistic in nature. Implementation of smart grids will allow demand to respond to the electricity market prices, hence the consumption pattern will change following the change of electricity prices over time. This causes uncertainty of amount of generation that should be delivered. Moreover, renewable energy output such as wind and solar power is heavily reliant on local weather (wind velocity and sunlight intensity) conditions, which are not easily predicted with high accuracy. These conditions result in a need for probabilistic analysis for the power system. As protection operation is influenced by power system quantities, it can be argued that stochastic analysis also needs to be applied for protection systems.

Furthermore, the deterministic techniques are often based on worst case scenario while the occurrence of the worst case condition is often very rare. Therefore it may not be helpful in decision making process.

2.8. Enhancement for the existing protection selection technique

A probabilistic selection approach is proposed to overcome the existing protection selection limitation and to anticipate future protection requirements. Although reliability analysis provides a probabilistic calculation technique, the method does not have the ability to rank the protection candidates or to find the optimum setting according to the protection overall performance (based on dependability, security, selectivity and speed). Reliability analysis can only rank the protection alternatives for each protection objective and hence cannot assist in finding the best protection candidate or an optimum setting. Moreover, results of reliability analysis are probabilities of failure modes in numbers with very small orders of magnitude which is often not convenient to be understood by decision makers.

Risk assessment on the contrary, can fulfil these requirements. Risk assessment quantifies the probabilities of the protection failures based on the protection characteristics, quantifies the consequences of the protection failures then calculate the risk as a product of the probability and value of the protection failure consequences. An example of risk assessment for power system protection selection process is shown in case study in chapter 7. The total risk assessment results of each protection alternative can be compared and ranked in order to find the best protection candidate or setting.

Risk assessment can also be used to measure whether the reduction of financial risk of the system faults due to utilization the protection scheme is comparable with the protection scheme cost. As although a robust protection scheme is always required for a power system however the cost of the protection equipment has to be considered.

2.9. Conclusion

Power system protection is an important component for a safe operation in a power system; hence an effective protection selection technique is needed to ensure that the best protection scheme or setting is chosen. The existing protection selection practices have limitations in finding the best compromise among the conflicted protection characteristics. Moreover, power system protection requirements will change in the near future due to implementation of new technologies in power systems. Also, the future power systems become more stochastic in nature due to implementation of renewable generation and smart grids. Therefore, an additional approach is needed to overcome the existing protection selection practices. The additional approach should able to find an optimum trade-off among protection characteristics, rank the protection alternatives and cope with the probabilistic nature of the power system. Risk assessment is proposed as a complement to the existing protection selection practices to find the best protection characteristic compromise. Risk assessment quantifies the protection failure mode probabilities and weights the protection characteristics according to their failure mode consequences. Hence the result can be used to find the best protection strategy for particular applications.

2.10. Reference for chapter 2

[1] C. R. Mason, "The art and science of protective relaying", Wiley, 1956.

[2] Y. G. Paithankar and S. R. Bhide, *Fundamentals of power system protection*. New Delhi: PHI Learning Private Limited, 2010.

[3] Alstom-Grid. (2011). *Network Protection & Automation Guide*. Available: http://www.alstom.com/grid/products-and-services/Substation-automation-system/protection-relays/Network-Protection-Automation-Guide-NEW-2011-Edition/

[4] Cigre-WG-A3.06, "Final report of 2004 - 2007 international enquiry on reliability of high voltage equipment.," Cigre, Paris2012.

[5] C. R. Heising and R. C. Patterson, "Reliability expectations for protective relays," in *Developments in Power Protection, 1989., Fourth International Conference on*, 1989, pp. 23-26.

[6] H. Kameda, S. Yoshiyama, G. Ushio, M. Usui, K. Sekiguchi, and C. Komatsu, "Estimation of replacement of numerical relay systems from reliability analysis," in *Advanced Power System Automation and Protection (APAP), 2011 International Conference on*, 2011, pp. 114-119.

[7] IEEE-SA, "IEEE std 493-2007 Recomendation Practice for the Design of Reliable Industrial and Commercial Power Systems," New York: IEEE, 2007.

[8] A. G. Phadke and J. S. Thorp, "Expose hidden failures to prevent cascading outages [in power systems]," *Computer Applications in Power, IEEE*, vol. 9, pp. 20-23, 1996.

[9] G. H. Kjolle, Y. Aabo, and B. T. Hjartsjo, "Fault Statistics as a Basis for Designing Cost-Effective Protection and Control Solutions," presented at the Cigre Paris, 2002.

[10] A. L. J. Janssen, I. Karakoc, M. J. M. v. Riet, and F. J. Volberda, "Simplicity Versus Complexity in Relation to the Reliability of Protection Schemes," presented at the Cigre general session 2008, Paris, 2008.

[11] "IEEE Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems (IEEE Buff Book)," *IEEE Std 242-2001 (Revision of IEEE Std 242-1986) [IEEE Buff Book]*, pp. 1-710, 2001.

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

[13] "Requirements for protection and control systems.Principles for the Icelandic power transmission network", v05, Landsnet Icegrid, 2011.

[14] "Application and Protection Setting Policy for the National Grid UK Transmission System," vol. PS(T)010-issue2, London: National Grid, 2011

[15] "Primary and Secondary Substations Protection and Control Equipment," issue no. 8, SP Power Systems Limited, 2004.

[16] E. E. Bernabeu, J. Thorp, and V. Centeno, "Methodology for a Security/Dependability Adaptive Protection Scheme Based on Data Mining," *Power Delivery, IEEE Transactions on*, vol. 27, pp. 104-111, 2012.

[17] S. Horowitz, A. G. Phadke, and B. Renz, "The Future of Power Transmission," *Power and Energy Magazine, IEEE,* vol. 8, pp. 34-40, 2010.

[18] V. Terzija, G. Valverde, C. Deyu, P. Regulski, V. Madani, J. Fitch, *et al.*, "Wide-Area Monitoring, Protection, and Control of Future Electric Power Networks," *Proceedings of the IEEE,* vol. 99, pp. 80-93, 2011.

[19] P. Zhang, K. Meng, and Z. Dong, "Probabilistic vs Deterministic Power System Stability and Reliability Assessment," in *Emerging Techniques in Power System Analysis*, Springer, 2010, pp. 117-145.

Chapter 3. Risk Assessment

In chapter 2, risk assessment has been proposed as an additional method to address limitations of the existing protection selection practices. Therefore, in this chapter, a risk assessment methodology that has been applied in many areas is introduced. The chapter starts with definition of the risk assessment process and then explains the generic steps of conducting risk assessment, data for risk assessment and implementation of the risk assessment results. The chapter also discusses the advantages and disadvantages of several well-known probability calculation techniques for use within risk assessment. Finally, some limitations of applying the generic risk assessment to power system protection are described .

3.1. Introduction to risk assessment

Risk, according to the Oxford Learner's Dictionary, is *the possibility of something bad happening at some time in the future; a situation that could be dangerous or have a bad result* [1]. Risk assessment is used to identify the causes of the dangerous event, finding out the consequences of the dangerous event and measuring whether or not the related risk is tolerable [2]. In other words, risk assessment is carried out to find answer of following questions [3]:

- What are the undesirable possibilities that may occur?
- How likely is it to happen?
- What are the consequences if it is happen?

From these questions, risk assessment is defined as a combination of likelihood and impacts of an accident.

There are two types of risk assessment: qualitative and quantitative risk assessment. A qualitative risk assessment describes all available information about the risk and concludes the likelihood of the risk event for any risk reduction strategy. Qualitative risk assessment usually carried out for condition when the risk is clearly unacceptable hence safeguards are needed whatever the magnitude [4]. Whereas for non-obvious risk, the magnitude of the risk needs to be measured therefore quantitative risk assessment is applied. Quantitative risk assessment measures the chance of a hazard transforming into reality and impact of the event in form of cost, death, index and etc. However, qualitative risk assessment can provide important contribution for quantitative risk assessment.

For power system protection, risk of protection failures is often non-obvious. For example, a failure of a distance protection to clear a fault in a transmission line may cause remote backup to operate, hence larger section of the line will be disconnected. This risk may acceptable if the consequences of the protection failure do not bring a cascading effect of the power system. Due to the non-obvious risk of protection systems, this thesis will focus on quantitative risk assessment hence the term risk assessment that used in this thesis will refer to quantitative risk assessment.

There are two well-known approaches to quantify and present the risk:

- Linear risk i.e. risk (*R*) is quantified and presented as probability occurrence of the accident (*F*) times its consequences (*C*) using formula [5]:

$$R = F \times C \tag{3.1}$$

- Pair of probability and consequences i.e. (*F*,*C*) which presented as a risk curve or risk profile [6, 7].

Linear risk provides a single value result while a risk curve is presented as a graph as shown in figure 3.1. In figure 3.1. the risk of curve A is higher than curve B and the risk of curve B is higher than curve C.

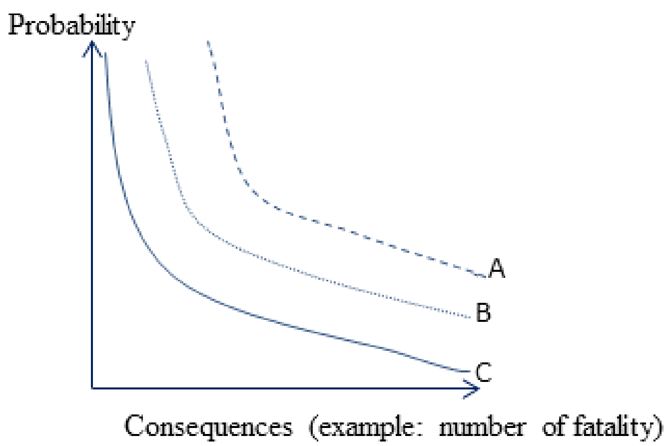

Figure 3.1. Risk curve

Linear risk approach is applied in insurance company in order to calculate insurance premiums [6]. However this approach is considered unsatisfactory in safety perception as one accident involving many fatalities can be quantified as having the same level of risk as a large number of accidents involving one or two fatalities. Therefore the risk curve approach is utilised for plant with fatality risk such as nuclear power station [6, 8], offshore platform [9], chemical industry [6] and spacecraft [10].

3.2. Risk assessment methodology

The basic steps of conducting risk assessment involve [5]:

a. Identification of the potential hazards.
b. Quantification of the consequences of each hazard.
c. Quantification of the probability of occurrence of each hazard.
d. Decision making based on the risk assessment results.

3.2.1. Identification of the potential hazard

Identification of potential hazard can be carried out using several approaches such as: checklists, Preliminary Hazard Analysis (PHA), Failure Mode and Effect Analysis (FMEA) or Failure Mode, Effect and Critical Analysis (FMECA), Hazard and Operability (HAZOP) Study, and Master Logic Diagram [5, 7]. A combination of FMEA and HAZOP is the most well-known approach to identify the initiating events of hazard.

The FMEA can be used as a first step to understand plant failures based on its component failures. This systematic analysis identifies all possible failure modes of each component of the system and analyses their effect to the system. Since FMEA finds system failure modes from component's failures, the system failure modes which are not caused by the components failures may be overlooked. Human operator errors, external event and multiple component failures are some examples of initiating event that cannot be identified using FMEA. A failure does not have to occur for a hazard be present in the system [11].

HAZOP (Hazard and operability) study is a systematic group approach to identify process of hazards and inefficiencies in a system [11]. The system is analysed using guide words which is used to quantify the intention and hence deviations. The list of guide words are No/Not, More, Less, As well as, Part of, Reverse, etc. Locations where process parameters can change or interfaces of functional areas are chosen as nodes. Then, HAZOP is carried out at each of the node. Limitations of HAZOP are: it requires amount of time to complete the intensive and tiring analysis, it cannot identify occupational hazards (electrical equipment, rotating machine etc.) and chronic hazards (chemical exposure, noise, etc.)[6]

Therefore, a combination FMEA and HAZOP can gives a more comprehensive analysis to identify potential[7]. FMEA identify failures caused by component failures and HAZOP can be applied to identify other initiating events.

3.2.2. Quantification of the consequences of each hazard

Event progression from initiating event to the unwanted consequences of the hazard can be traced using an event tree. The consequences of each hazard are assessed using any possible development scenario. The consequences of accidents can be considered in three types [5]:

- Individual consequences for people who work in the plant
- Community and environment consequences because of damage or pollution outside boundary of the plant
- Economic consequences arise from loss of capital assets, production and compensation.

An example of an event tree is shown in figure 3.2. It shows the accident progression of an important transmission line loss. The quantities in the figure are for examples, the real conditions could change. The accident causes varying consequences depending on how successful accident mitigation. If all mitigation actions are successful, then minimum load shedding (15% of total system load for 0.5 hour) will occur. Different percentages of load shedding and durations can occur for each failure of the mitigation action. The worst condition when all the mitigation actions fail then total blackout for seven hours cannot be avoided.

Transmission	Emergency power	Load Shedding	Automatic Islanding	Percentage load shedding and duration (hours)

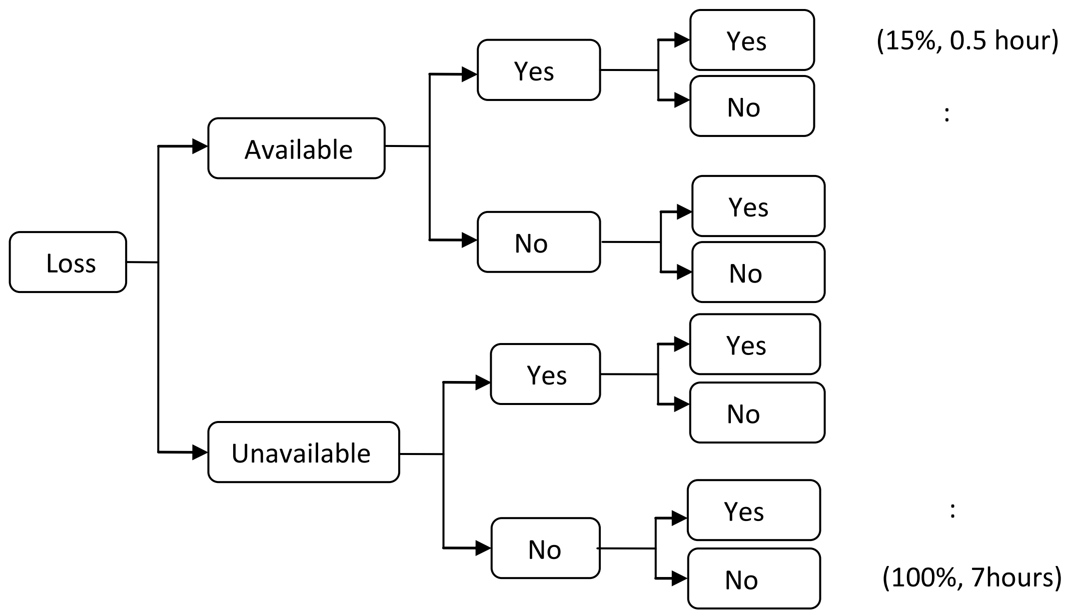

Figure 3.2. Event tree for consequences of a transmission loss [12]

3.2.3. Quantification of the probability occurrence of each hazard

For each hazardous event that has been found in consequences analysis, the probability of its occurrence needs to be calculated. There are several techniques to calculate the probability of the hazardous event such as fault tree analysis, Markov chain, Monte Carlo simulation and Bayesian Networks.

3.2.3.1. Fault tree analysis

Fault Tree (FT) analysis is the most widely used method for evaluation of large, safety-critical system [5,13,14]. FTs provide graphical and mathematical representations which are convenient to use and to communicate the result of the analysis. The construction of a fault tree is started from the top event, which is the considered system failure mode. Since there are many possible failure modes in a system, hence more than one fault tree maybe constructed for assessing the system. The causes of the top event can be represented as branches of the top event. The fault tree is developed further by continually identified causes of the events until basic events are encountered. Analysis of the fault tree is carried out using basic event probabilities data.

An example of fault tree diagram is shown in figure 3.3. The diagram consist of two basic elements i.e. gates and events. AND and OR gates shows the relationship between events to represent higher level events. The output of a AND gate will be true if all of its input are true. As for an OR gate, the output will be true if at least one of its input is true.

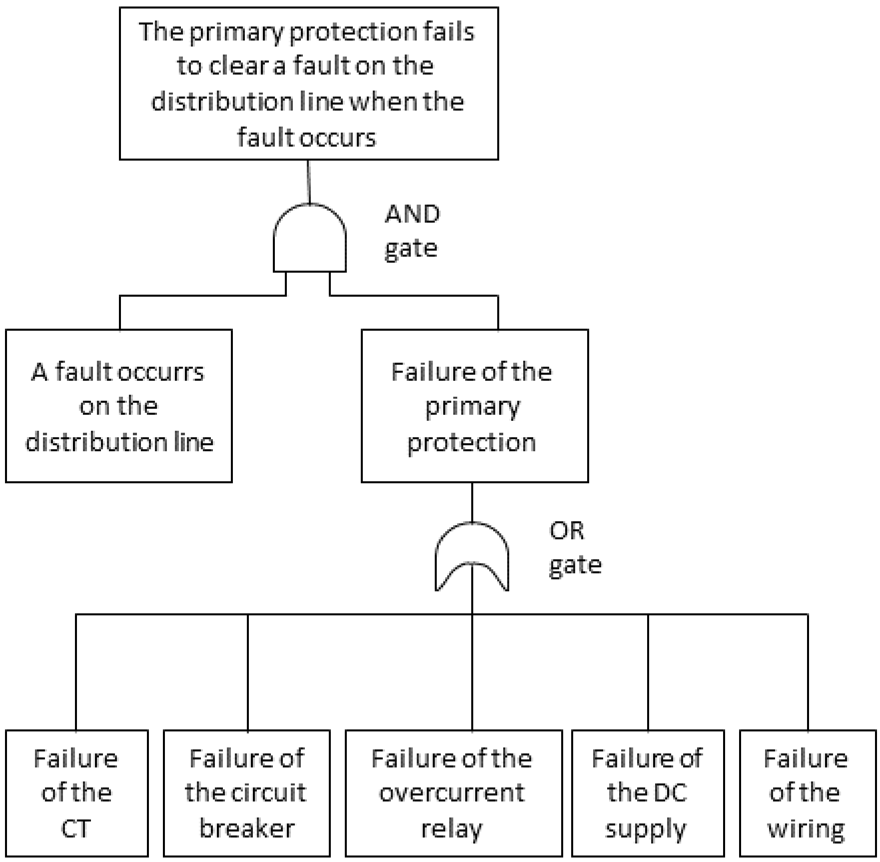

Figure 3.3. A fault tree of overcurrent protection failure

The probability of the occurrence of the top event is calculated using Boolean algebra from the probability of the basic events. For fault tree in figure 3.3, probability of the top event can be calculated as follows:

$$P(TE) = P(line)\, P(prot)$$

Since $P(prot) = P(CT) + P(relay) + P(CB) + P(DC) + P(wiring)$

$$\overline{P(prot)} = \overline{\mathrm{P(CT) + P(relay) + P(CB) + P(Battery) + P(wiring)}}$$

$$\overline{P(prot)} = \overline{P(CT)} \times \overline{P(relay)} \times \overline{P(CB)} \times \overline{P(DC)} \times \overline{P(wiring)}$$

$$P(prot) = 1 - (\overline{P(CT)} \times \overline{P(relay)} \times \overline{P(CB)} \times \overline{P(DC)} \times \overline{P(wiring)})$$

$$P(prot) = 1 - [(1 - P(CT)) \times (1 - P(relay)) \times (1 - P(CB)) \times (1 - P(battery)) \times (1 - P(wiring))]$$

Hence

$$P(TE) = P(line)\{1 - [(1 - P(CT)) \times (1 - P(relay)) \times (1 - P(CB)) \times (1 - P(battery)) \times (1 - P(wiring))]\} \quad (3.2)$$

Where :

P(TE) = probability of Top Event i.e. Primary protection fails to clear a fault in the distribution line when the fault occurs

P(line) = probability of occurrence of a fault on the distribution line

P(prot) = failure probability of the primary protection

P(CT) = failure probability of the current transformer

P(relay) = failure probability of the overcurrent relay

P(CB) = failure probability of the circuit breaker

P(DC) = failure probability of protection's DC supply

P(wiring)= failure probability of the protection wiring

Although it is the most frequently used methods, FT has some weaknesses that prevent it from being applied in specific systems. The weaknesses come from the assumption which is used to develop FT methodologies [13]:

a. States of the variables are binary (working/not-working).
b. Events are statistically independent.
c. Relationship between events and causes are represented by simple gate (AND, OR, XOR, etc.) which give limited possibility in modelling the system.

3.2.3.2. Markov analysis

Markov analysis is an important technique that can overcome the drawback of the FT analysis. Markov analysis can be applied to multi state variables. It is also able to represent dependent failures, such as standby redundancy and common cause failures. In addition, Markov analysis can provide solution for the time dependant probabilities [5].

Basic modelling concepts of Markov approach is illustrated in fig. 3.4, for a two-state system. State 1 is a working state, state 2 is a failed state, λ is the failure rate and μ is the repair rate. Transition probability matrix of the system:

$$P = \begin{bmatrix} 1-\lambda\,\Delta t & \lambda\,\Delta t \\ \mu\,\Delta t & 1-\mu\,\Delta t \end{bmatrix}$$

The limiting state probabilities:

$$[\boldsymbol{P_1} \quad \boldsymbol{P_2}]\begin{bmatrix} 1-\lambda\,\Delta t & \lambda\,\Delta t \\ \mu\,\Delta t & 1-\mu\,\Delta t \end{bmatrix} = [\boldsymbol{P_1} \quad \boldsymbol{P_2}]$$

With $\boldsymbol{P_1} + \boldsymbol{P_2} = 1$

Solving these equations give:

$$\boldsymbol{P_1} = \mu/(\lambda + \mu) \tag{3.3}$$

$$\boldsymbol{P_2} = \lambda/(\lambda + \mu) \tag{3.4}$$

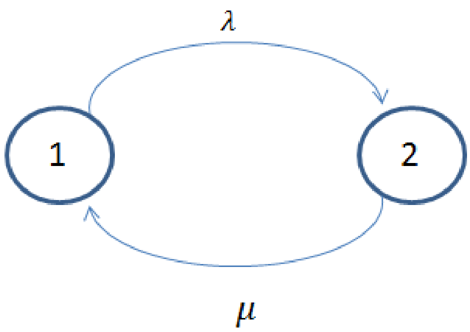

Figure 3.4. A single component repairable system

Markov analysis only works for components that have constant failure and repair rates which means it is strictly applicable only for random variable with exponential distribution. Another disadvantage of this method is the difficulty for large system. For systems with N components where each component has two states, the number of system states is 2^N. The size of the problem grows exponentially with the number of the components and states hence it can cause difficulties in calculation.

3.2.3.3. Monte Carlo simulation

Monte Carlo Simulation is a more powerful method, because it overcomes FT and Markov problems. This method is also suitable for very large or complex systems [15]. The Monte Carlo simulation technique replicates the system behaviour by studying interaction among its components. The simulation is carried out on a computer as a statistical experiment. Millions of hours of life cycle of each system component are simulated. The simulation is carried out by generating random numbers and converting these random numbers into time to failures and time to repairs of the component being examined according to the statistical distribution parameter.

The steps for Monte Carlo simulation are as follows [21]:

1) Generate a random number for a component operating time using its statistical distribution parameters
2) Generate a new random number for a repair time using its statistical distribution parameters

3) Add result 1 and 2 to make a life cycle
4) Repeat step 1-3 for a period of operating life
5) Repeat step 1-4 for each component
6) Compare sequence of each component and calculate system failure durations, frequencies and other parameters
7) Repeat steps 1-6 for a desired number of simulations

The life cycle of the system is graphically shown in Fig. 3.5 for 3 components connected in parallel and in Fig. 3.6 for 3 components connected in series. Parallel and series connections here are taken from the reliability point of view. In a parallel connection, system only can fail if all of components fail at the same time, whereas in a series connection, a system will fail if at least one of the components fails. For parallel components in Fig.3.5, a down state of the system is from time a (*t*=*a*) to time b (*t*=*b*), where all the components are in down state. For series components in Fig. 3.6, three down states are found: c-d, e-f and g-h.

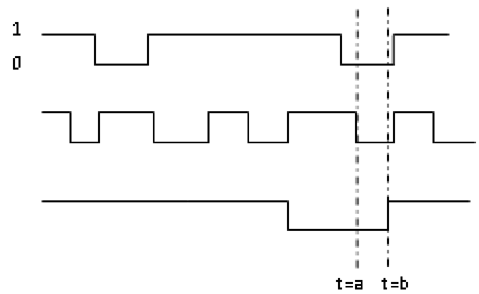

Figure 3.5Life cycles of 3 components connected in parallel

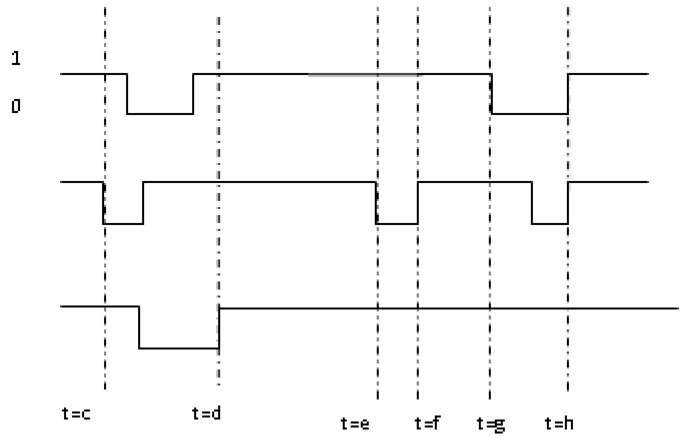

Figure 3.6. Life cycles of 3 components connected in series

The limitation of this method is:

a. long computation time
b. requires data of statistical distributions with their parameters which is often difficult to be obtained.

3.2.3.4. Bayesian Network

Bayesian networks are a technique for representing and analysing models involving uncertainty. This probability calculation technique has been used in many applications and can be broadly categorized in two main groups: predictive analysis and diagnostic analysis [13].

Bayesian networks include both qualitative and quantitative types of analysis [13]. The qualitative part consists of directed acyclic graphs representing logical relationships between variables. A simple example of the directed acyclic graph is presented in figure 3.7. The arrows which link the nodes in the graphs represent causal dependence between the random variables that they are connecting i.e. from a cause to an effect. Nodes with outgoing arrows are termed parents and the nodes with incoming arrows are termed descendants. Nodes without any parents are termed root nodes. The quantitative part consists of prior probability of root nodes and Conditional Probability Tables (CPT) of other nodes. Prior probabilities at the root nodes represent probability occurrences of the states of the root nodes, while the

CPTs represent occurrences probability of the child node states given all parent states.

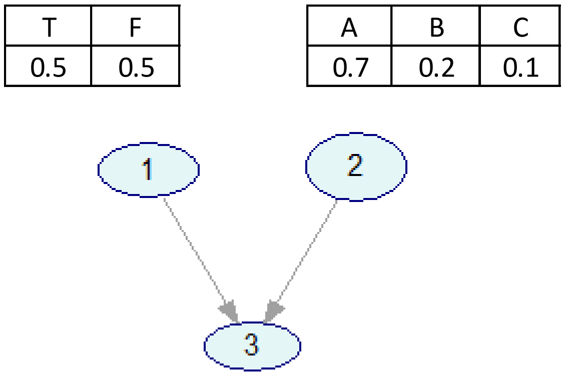

Figure 3.7. A graph of a Bayesian network and their prior probabilities

Table 3.1. The Conditional Probability Table (CPT) of node 3 in Figure 3.7

Node 1	T			F		
Node 2	A	B	C	A	B	C
G	1	0.5	0.2	0	0.9	0.5
H	0	0.3	0.3	0.5	0.1	0.5
J	0	0.2	0.5	0.5	0	0

Each node can have two or more states. For example in figure 3.7, node 1 has two states (T and F), whereas node 2 has three states (A, B and C). The probability of occurrence of each state for node 1 and 2 is shown in probability tables in figure 3.7. The probabilities of occurrence of node 3 states are based on the CPT presented in table 3.1. A CPT shows conditional probability of state occurrences based on its parent states. From table 3.1 for example, if it is known that node 1 is in state F and node 2 is in state B, then probabilities of having node 3 in states G, H and J are 0.9, 0.1 and 0 respectively. The sum of probabilities for all states is always one.

Probability of occurrence of a descendant x is based on total probability of all its parents states (y_i):

$$P(x) = \sum_i P(x|y_i)P(y_i) \tag{3.5}$$

For example, probability of node 3 (N3) being in state H is calculated as the total product of its conditional probability and the parent states in node 2 (N2) and node 1 (N1):

$$P(N3 = H) = \sum_i P(N3 = H|parents\ of\ N3_i)P(parents\ of\ N3_i)$$

$$P(N3 = H) = P(N3 = H \,|\, N1 = T, N2 = A)P(N1 = T)P(N2 = A) + P(N3 = H \,|\, N1 = T, N2 = B)P(N1 = T)P(N2 = B) + P(N3 = H \,|\, N1 = T, N2 = C)P(N1 = T)P(N2 = C) + P(N3 = H \,|\, N1 = F, N2 = A)P(N1 = F)P(N2 = A) + P(N3 = H \,|\, N1 = F, N2 = B)P(N1 = F)P(N2 = B) + P(N3 = H \,|\, N1 = F, N2 = C)P(N1 = F)P(N2 = C)$$

$$P(3 = H) = 0 + (0.3 \times 0.5 \times 0.2) + (0.3 \times 0.5 \times 0.1) + (0.5 \times 0.5 \times 0.7) + (0.1 \times 0.5 \times 0.2) + (0.5 \times 0.5 \times 0.1)$$

$$P(3 = H) = 0.255$$

The advantages of employing Bayesian Networks are ability to use multi-states variables, unlimited cause and effect relation models, ability to represent dependent variables and ability to cope with limited available statistical data.

3.2.3.5. Comparison of the probability calculation techniques

Although giving similar probability results, each of the probability calculation techniques has its own advantages and disadvantages. Summary of the strength and limitation of the four techniques are shown in table 3.2.

When conducting risk assessment, the choice of probability calculation technique is based on the nature of the assessed system. If there are many states for example, then clearly FT will not be the most appropriate technique. Otherwise, more calculation effort is required as more models of separate FTs are needed.

Table 3.2. Comparison of the probability calculation techniques

Feature	Fault Tree	Markov	Monte Carlo	Bayesian Network
State of variable	two	unlimited	unlimited	unlimited
Conditional probability model of cause and effect	limited	unlimited	limited	unlimited
Modelling of dependent variables	not straightforward	straightforward	straightforward	straightforward
Need of data	simple probabilities	only for exponential distribution in term probability or frequency	detail of probability distribution types and their parameters	a simple probabilities
Calculation time	medium	long for large system	long	medium
Applicability for large system	yes	no	yes	yes
Graphical presentation of the calculation model	good	poor for large system	no presentation	good

3.2.3.6. Metrics of Risk Assessment

There are several metrics that can be used to quantify the probability of the hazardous event i.e. [5,7]:

- Unreliability is a time-dependant probability which addresses the probability of the occurrence of the first failure in the considered mission time.

- Unavailability is a time-independent probability which defines the percentage of time that the system is not in an operating condition.
- Failure density is a time-dependant probability which address the probability of the occurrence of the first failure exactly at the end of the mission time.
- Failure intensity, or failure rate, is the number of occurrence of failures for a mission time.
- Mean time to failure is the expected duration to failure from the first use/after repairs.
- Failure duration.

However, metrics for the hazardous system which can be calculated using all probability calculation techniques are unreliability and unavailability. This two parameters are important parameter in reliability analysis of electrical equipment in critical facility [16]. Unreliability can be calculated using equation (3.6) while unavailability using equation (3.7).

$$F = 1 - e^{-\lambda t} \tag{3.6}$$

$$U = \frac{MTTR}{MTTF + MTTR} \tag{3.7}$$

Where

F = unreliability

λ = failure rate (failure/year)

t = mission time the concerned duration of the assessment (year, day, etc.)

U = unavailability

$MTTR$ = main time to repair (hour)

$MTTF$ = main time to failure (hour)

3.2.3.7. Data sources of Risk Assessment

Data collection is an important part of risk assessment studies. The required data for the study depends on the applied probability calculation technique. They could be failure and repair rates of the system components, statistical distribution types and its parameters, probability of event occurrences, main time to failure, down time, etc.

There are three sources of data [5] :

- In-service historical data

Data is collected from operating plant in form of failure report, repair/replacement action report of the components/equipment. The failure–repair event data is taken from similar equipment or from a single item of equipment. The restoration is assumed ‘as good as new’ which mean each repair is perfect. The reports are analysed to generate convenient data for the risk assessment

- Generic data

In risk assessment for new design of equipment, data are taken from broadly similar equipment operating under similar function and environment conditions. Data can be taken from data banks, handbooks, private or published data tables. However, in general, in-house data bank provide better data quality than published data tables[5].

- Expert opinion [18]

For new equipment or very reliable components, failure data are seldom available and often impossible to be observed. Therefore, expert opinion is a useful technique for constructing and quantifying models. Expert opinion data may also be used to refine estimates from real data when model of the data is not as fine as required. Some problems of using expert opinion may arise, such as choosing the correct experts and biases of data/opinions.

From those three sources of data the accuracy levels are consecutively reduced from the former to the latter.

3.2.4. Decision making based on the risk assessment results

Risk assessment results can support decision making process in anticipation of risks and uncertainties. There are several theories for risk assessment based decision making such as cost-benefit analysis, risk acceptability criteria and ALARP (As Low As Reasonably Practicable) approach [22].

Cost-benefit analysis evaluates the benefit of employing a project, plant or policy and the cost that need to be paid. The analysis converts all benefits and costs into a monetary value then calculates the expected monetary value as total benefit minus total cost. One element of the cost is the risk. The decision is based on the maximum expected monetary value.

Risk acceptability criteria are usually established in plant or projects which have safety issues either for workers, the public nearby the plant or the environment. The risk result must be below specific acceptability criteria in order for the project or plant to be approved. The criteria may be in the form of individual safety standards for workers or public [17] or effect to environment [9]. If the risk is beyond acceptable criteria hence the project will be rejected or the plant’s design will be modified to reduce the risk. An example of risk acceptability criteria of the environment spill risk from offshore oil and gas platform which is developed by Norwegian authority in [9] is shown in table 3.3. It is shown that for more significant damage level of accidents, the acceptable accident frequency is greatly reduced. However in [22] the authors argue that risk acceptable criteria drives industries to only achieve the minimum level of risk (within the criteria) without encouraging them to seek alternatives with better risk profiles.

Table 3.3. Acceptance criteria for environment spill risk [9]

Damage category	Average recovery	Acceptable frequency limit
Minor	½ year	< 1 event per 10 years
Moderate	2 years	< 1 event per 40 years
Significant	5 years	< 1 event per 100 years
Serious	20 years	< 1 event per 400 years

The ALARP approach is considered better than risk acceptability criteria [9, 22] because it forces the industry to find lower-risk alternatives except if the cost of the alternative is a lot higher than the reduced risk. ALARP approach consists of three level of risk i.e.:

- Very low risk hence it can be negligible (broadly acceptable risk)
- Intermediate risk, risk need to be reduced As Low As Reasonably Practicable (ALARP)
- Very high risk that cannot be accepted.

The UK safety regulator, Health and Safety Executive (HSE), employs the ALARP approach for individual, worker or public safety [23].

3.3. The requirement for a framework for power system protection risk assessment

The existing protection schemes and setting selection policies [24-27] do not reflect implementation of risk assessment to complement the selection process. Pure deterministic approaches are often applied such as in guidelines for assessing the impact of DG upon distribution network protection coordination [28]. However, the pure deterministic approaches may not be effective for the selection process due to an inability to find optimum compromises among the conflicted protection objectives i.e. dependability, security, selectivity and speed. In references [24-26], the protection scheme and setting selection processes are comprehensive, but mostly based on engineering judgments and experiences which may not be fully quantified or justified. This practice may not be applicable for future power system conditions.

Risk assessment is suggested as a complement to the existing protection selection methods: it can compare the protection schemes or settings according to their levels of risk in order to find the best compromise that satisfies the protection objectives. Furthermore, the future power system tends to be more stochastic in nature due to implementation of smart grid technology and renewable generation; consequently the probability based, data based, quantitative risk based approaches can assist in defining and refining the various aspect of protection selection, assessing the existing protection in the future and setting selection.

The generic risk assessment methodology provides numerous ways of conducting the assessment. However, effective and efficient ways of conducting risk assessment for certain system/plant depend on the nature of the plants. Therefore, a framework of risk assessment which is dedicated for a certain area is needed. Several risk assessment frameworks have been established for specific fields such as in maritime transportation [19], space travel [10], nuclear power plant [6, 20] and offshore oil and gas platforms [9]. The framework for maritime transportation in [19] addresses the risk-based design of ship operation, where ship designs contribute to the likelihood of the ship damage levels, capsizing and amount of life loss following a collision. The framework for space travel risk in [10], which is released by NASA, focuses on the probability of aerospace mission failure, loss of crew or vehicle from a specific mission and large capital loss. For nuclear power plant [6, 20], the risk assessment framework contributes to decision making regarding reactor design, operation and location according the standard of safety goals. The risk assessment framework in [9] addresses hazards of fire, explosion, collision and falling objects to personnel safety, environment and material damages. All of this frameworks focuses on the specific risk on the particular field hence they are very practical. However, for power system protection area, risk assessment is still not common to be applied and there is no dedicated risk assessment framework has been compiled.

A risk assessment framework assists in producing a systematic and complete risk assessment report. It also helps the decision maker who will use the assessment result in understanding the risk of utilisation of a particular protection scheme. Moreover, a dedicated framework can avoid inconsistency in power system protection risk assessment, absence of good documentation of the assessment and false quantification. Although the framework cannot guarantee the accuracy of the risk assessment results, it will disclose the reasons for differences between two risk assessment results for the same protection schemes for the same protected system. It may come from different intended use of the assessment, different metrics, different scenarios, different assumptions, etc. For these reasons, this thesis proposes a dedicated framework for power system protection which will be explained in more detail in chapter 4.

3.4. Conclusion

Risk assessment has been a well-known method for analysing the risks associated with a system, plant or design. This systematic assessment is started from identification of potential hazards and culminates with implementation of the risk result for decision making. As a of decision making tool, risk assessment can be applied in power system protection as a complement to existing power system protection selection techniques. However, since there are many ways of conducting a risk assessment, an efficient and dedicated framework for power system protection risk assessment is essential. The framework will assist in conducting the risk assessment efficiently and will guide in reporting the assessment result systematically to prevent misinterpretation by decision makers.

3.5. References for chapter 3

[1] (2014, 25 June). *Oxford Learner's Dictionary*. Available: http://www.oxfordlearnersdictionaries.com/definition/english/risk_1

[2] M. Rausand, *Risk Assessment: Theory, Methods, and Applications*: Wiley, 2013.

[3] S. Kaplan and B. J. Garrick, "On The Quantitative Definition of Risk," *Risk Analysis*, vol. 1, pp. 11-27, 1981.

[4] WHO and FAO, "Risk Characterization of Microbiological Hazards in Food, Guidelines," *Microbiological Risk Assessment Series*, United Nation, 2009. Available: http://www.who.int/foodsafety/publications/micro/MRA17.pdf

[5] J. D. Andrews and T. R. Moss, *Reliability and Risk Assessment*, second ed. London: Professional Engineering Publishing, 2002.

[6] R. R. Fullwood, *Probabilistic safety assessment in the chemical and nuclear industries*, 2 ed. Woburn: Butterworth-Heinemann, 2000.

[7] H. Kumamoto and E. J. Henley, *Probabilistic Risk Assessment for Engineers and Scientists*, second ed. New York: IEEE Press, 1996.

[8] NUREG, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plant," U.S. Nuclear Regulator Commission, Washington DC1990.

[9] J.-E. Vinnem, *Offshore risk assessment: principles, modelling and applications of QRA studies*: Springer, 2007.

[10] M. Stamatelatos and H. Dezfull, *Probabilistic Risk Assessment Procedures Guide for Nasa Manager and Practitioners*. Washington, DC: NASA, 2011.

[11] N. J. Bahr, *System Safety Engineering and Risk Assessment*. Washington: Taylor & Francis, 1997.

[12] O. Gjerde, G. Kjolle, N. K. Detlefsen, and G. Bronmo, "Risk and vulnerability analysis of power systems including extraordinary events," in *PowerTech, 2011 IEEE Trondheim*, 2011, pp. 1-5.

[13] A. Bobbio, L. Portinale, M. Minichino, and E. Ciancamerla, "Improving the Analysis of Dependable Systems by Mapping Fault Tree into Bayesian Networks," *Reliability Engineering and Safety,* vol. 71, pp. 249 - 260, 2001.

[14] H. Boundali and J. B. Dugan, "A Discrete-time Bayesian Network Reliability Modelling and Analysis Framework," *Reliability Engineering and Safety,* vol. 87, pp. 337-349, 2005.

[15] D. Vose, *Quantitative Risk Analysis: A Guide to Monte Carlo Simulation Modelling*. Chichester: John Willey & Sons, 1997.

[16] IEEE-SA, "IEEE std 493-2007 Recomendation Practice for the Design of Reliable Industrial and Commercial Power Systems," New York: IEEE, 2007.

[17] COMAH. (06/02/2013). *Risk analyses or 'predictive' aspects of comah safety reports guidance for explosives sites*. Available: http://www.hse.gov.uk/comah/assessexplosives/step5.htm

[18] T. Bedford and R. Cooke, *Probabilistic Risk Analysis: Foundations and Methods*. Cambridge: University of Cambridge, 2001.

[19] J. Montewka, S. Ehlers, F. Goerlandt, T. Hinz, K. Tabri, and P. Kujala, "A framework for risk assessment for maritime transportation systems—A case study for open sea collisions involving RoPax vessels," *Reliability Engineering & System Safety,* vol. 124, pp. 142-157, 4// 2014.

[20] *IAEA Safety Standart Series, Safety Assessment and Verification for Nuclear Power Plants*, Safety guide No. NS-G-1.2 , IAEA, 2001.

[21] R. Billinton and R. N. Allan, *Reliability Evaluation of Engineering System: Concepts and Techniques*, second ed. New York: Plenum Press, 1992.

[22] T. Aven and J. Vinnem, "Risk management, with applications from the offshore oil and gas industry," *NY: Springer Verlag*, 2007.

[23] COMAH. (06/02/2013). *Risk analyses or 'predictive' aspects of comah safety reports guidance for explosives sites*. Available: http://www.hse.gov.uk/comah/assessexplosives/step5.htm

[24] "Requirements for protection and control systems.Principles for the Icelandic power transmission network", v05, Landsnet Icegrid, 2011.

[25] "Application and Protection Setting Policy for the National Grid UK Transmission System," vol. PS(T)010-issue2, London: National Grid, 2011

[26] "Primary and Secondary Substations Protection and Control Equipment," vol. issue no. 8, SP Power Systems Limited, 2004.

[27] "IEEE Guide for Protective Relay Applications to Transmission Lines," *IEEE Std C37.113-1999*, p. i, 2000.

[28] T. K. Abdel-Galil, A. E. B. Abu-Elanien, E. F. El-Saadany, A. Girgis, Y. A. R. I. Mohamed, M. M. A. Salama, *et al.*, "Protection Coordination Planning with Distributed Generation," Natural Resources Canada (NRCan), Waterloo2007.

Chapter 4. A Framework for Risk Assessment of Power System Protection

As mentioned in chapter 2, current practices of selecting protection schemes have limitations in finding optimum trade-off between dependability, security, selectivity and speed of operation. Moreover, development of new technologies will bring changes in power system conditions and performance hence it requires protection schemes that might be very different from those which already exist for example wide area measurement based protection and adaptive protection. As a consequence, no past practices will be available to guide the choice of the most appropriate protection scheme. Futhermore, future power system technology trends i.e. renewable generation (wind and solar) and smart grids will increase the probabilistic nature of power systems. Therefore, risk assessment is considered as an additional approach that can assess the performance of protection schemes.

In order to provide guidance for the assessors who conduct the protection risk assessment and the decision makers who use the risk assessment results, a framework for power system protection risk assessment has produced. The assessors are assisted in choosing the efficient methodologies for conducting the risk assessment and producing a systematic risk assessment report. The decision makers, on the other hand, are guided into better understanding of the value of the risk assessment report.

The framework is developed based on the generic risk assessment methodology as presented in chapter 3, as well as considering the nature of power system protection. The framework focuses on power system protection related risk and it is very practical to this field which cannot be found in the risk assessment frameworks used in other fields. The application of the protection risk assessment can be also extended to other protection design related purposes such as evaluation of the existing schemes or finding optimum protection settings.

4.1. The proposed risk assessment framework

The framework for power system protection risk assessment consists of problem definition (reasons, intended use and scope of the risk assessment), terminologies and metrics, knowledge of the protection and the protected system, system scenarios, data and assumptions, the risk assessment steps and decision making. Each component of the framework should be provided in the risk assessment report. The schematic diagram of the framework is shown in figure 4.1.

From figure 4.1, system scenarios are developed from outcomes of other elements of the framework i.e. the element of reason, intended use and scope of the assessment, the element of knowledge of the protection and the protected system, and the element of terminology and metrics. The element of data and assumptions contributes to the system scenarios, conversely the adopted scenarios may also contribute to the required data/assumption in the assessment.

From the system scenarios in figure 4.1, the elements of the risk assessment steps are developed. The steps start from identification of the protection failure modes to sensitivity analysis. For each of the identified protection failure modes, the consequences of the failure modes should also be identified. If the consequence of a failure mode is not significant and can be ignored, the particular failure mode can be excluded from the assessment. The next step is to identify the initiating events of the failure modes. Then, the risk models can be constructed based on the failure modes, initiating events of the failure modes, consequences of the failure modes and system scenarios. The risk models are utilised to quantify the probability of failure mode consequences. The magnitudes of the consequences also require to be quantified, which are based on the costs of undesired consequences. The risk models require to be validated to ensure correct calculation of the probability results. The following step is quantification of the risk. Risk is quantified as a product of the likelihoods and the magnitudes of failure modes consequences. Finally, sensitivity analysis is carried out as an additional validation of the risk assessment. The risk results become an input for subsequent decision-making processes.

Detail of each framework element is explained in the rest of this chapter.

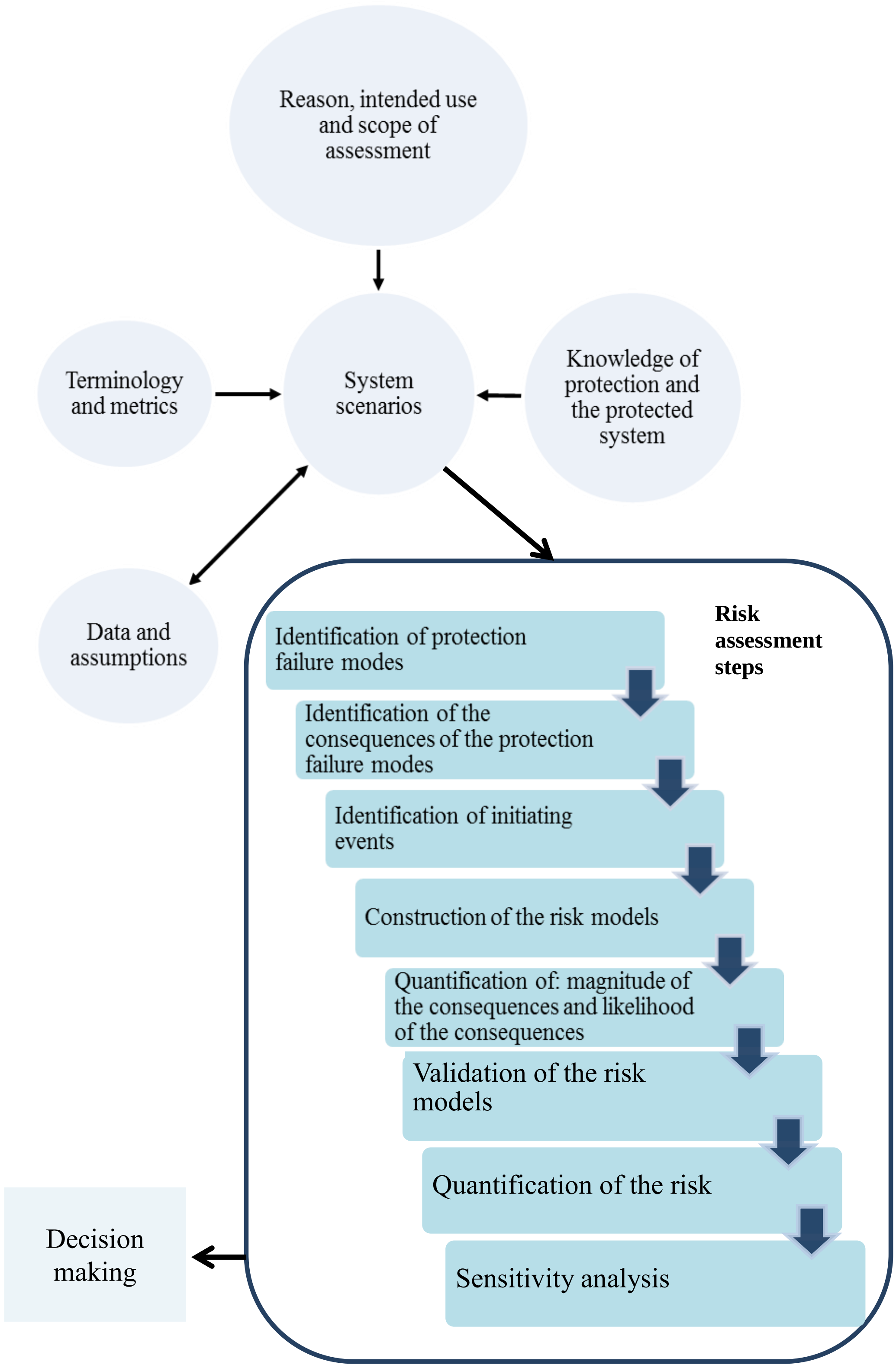

Figure 4.1. The schematic diagram of the framework for power system protection risk assessment

4.2. Reasons, intended use and scope of the assessment

The reasons for conducting, the intended use and scope of the risk assessment must be explained at the beginning of the report so the reader will understand the value and limitations of the risk assessment result. The explanation includes why risk assessment is carried out, how the assessment results will be used, in which condition that results can be used, cannot be used or can be used with caution. Risk assessment is usually carried out for the useful life phase of the protection system (and also the protected system) where the failure rates of the components are constant. However, depending on the intended use, it is also possible that the assessment scope is during “early life” or “wear out” phase of the protection system lifecycle.

4.3. Terminology and metrics

As mentioned in section 3.1., a risk assessment can be quantified and reported either in the form of a linear risk or a risk curve. For power system protection risk assessment, the linear risk is considered most suitable due to the following reasons:

- The main focus of protection risk assessment is finding the best compromise of the overall performance in term of protection dependability, security, selectivity and speed; therefore a single value result from the assessment is a convenient way to find optimum setting or to rank the candidates.
- Two probability metrics are involved for the protection risk assessment i.e. frequency and duration of the failure consequence, therefore if the risk curve approach is employed, two risk curves are needed. This results in a higher burden for decision making process as more curves need to be considered.
- Human fatality risk due to power system protection failure modes is often very rare. If it occurs, it only involves a small number of workers (usually one person). Therefore risk curve with consequences of number of fatalities will not be relevant.

Since the risk assessment for power system protection will adopt linear risk for the risk quantification, the framework will be based on this type of risk assessment. This terminology of risk assessment must be explained at the beginning of the assessment report.

Metrics that are used in quantification require to be explained in term of their definition and units. Regarding consequences of the protection failure modes (i.e. power system element disconnection as described in section 4.13.) the frequency and duration of disconnection are the two important metrics for protection risk assessment. If the failure rate λ is small, the unreliability F in equation (3.6) can be approximated as in equation (4.1).

$$F \cong \lambda \times t \tag{4.1}$$

Using a unity mission time (t =1) for equation (4.1) unreliability can be a measure of failure frequency.

$$F \cong \lambda \tag{4.2}$$

The expected duration of the disconnection can be measured using unavailability U as in equation (4.3)

$$d = U \times t \tag{4.3}$$

Where

d = expected duration of disconnection of a particular element of the power system in a mission time (hour/year or hour/day)

U = unavailability due to disconnection of a particular element of the power system

t = the mission time (year, day, etc.)

The mission time for a component should be smaller than its Mean Time To Failure (MTTF), because unreliability is the probability of occurrence of first failure (or next failure after a repair). A longer mission time than MTTF will result in imprecisely probability. Therefore, the choice of the system mission time is based on the smallest MTTF of the initiating events of failure modes and the protection risk results will be expressed in this selected mission time.

However, the application of equation (4.3) for the expected disconnection duration due to protection failure modes can only be applied on radial networks. For non-radial network, the disconnected element can be back into services as soon as possible through other branch of the network. The disconnection duration is not entirely determined by the causes of the disconnection i.e. protection failure mode.

Therefore, for non-radial network, the expected disconnection duration is quantified from historical data of similar disconnected element:

$$d = F \times t_s \tag{4.4}$$

Where

d = expected duration of disconnection in a mission time (hour/year or hour/day)

F = probability occurrence (unreliability) of the disconnection (per year or day)

t_s = historical disconnection duration (hour)

The duration in equation (4.3) should be equal with equation (4.4) if the mission time in equation (4.3) is a unit time for example a year, a day, etc. as follows.

For unavailability:

$$U = \frac{MTTR}{MTTF + MTTR}$$

$$as\ MTTR \ll MTTF$$

$$U \cong \frac{MTTR}{MTTF} \tag{4.5}$$

$$MTTF = \frac{1}{\lambda} \tag{4.6}$$

(4.6)&(4.5)

$$U = \frac{MTTR}{1/\lambda} \tag{4.7}$$

(4.3)&(4.7)

$$d = U \times t = \frac{MTTR}{1/\lambda} \times t$$

$$d = MTTR \times \lambda \times t \tag{4.8}$$

For unreliability:

(4.1) & (4.3)

$$d = F \times t_s = \lambda \times t \times t_s \tag{4.9}$$

Since

$$t_s = MTTR \tag{4.10}$$

(4.8) & (4.9)

$$d = MTTR \times \lambda \times t \tag{4.11}$$

It can be seen that expected duration in equation (4.3) is equal with duration in equation (4.4) as shown in equation (4.8) and (4.11) if the mission time is unity. Therefore, unity mission time is used for protection scheme risk assessment.

4.4. Knowledge of the protection system and its protected system

Collecting the information about the protection system and its protected system is an important stage in understanding the system being assessed. The protected system information may be in terms of the protected system layout and components, other protection devices installed in the system, working principles of components of the protected system, variation of the system condition and behaviour during abnormal condition (for example during protection failure modes). For the protection system, the information consists of protection system components with their failure modes, protection working principles, settings, etc.

4.5. System scenarios

Scenarios identification of the protected system is an important part of the risk assessment process. The scenario identification tries to answer the following questions:

- What variation of primary system condition can occurs?
- Which primary system conditions can cause each protection failure mode?
- What will happen following each protection failure mode for a given primary system condition?

Since there are many variations of the primary system condition as well as types and positions of the faults, these result in multi-scenario assessments. These multi-scenarios are generated based on cause-effect sequences of events. Sequences of scenarios can be illustrated as in figure 4.2. Several initiating events (I_1 to I_n), such as protection component failures, occurrence a fault or other power system condition, cause failure modes 1 or failure mode 2 of the protection. The final consequences of the protection failure modes vary according the primary system condition, fault conditions and also the protection condition. The final consequences (C_1, C_2,…, C_n) may be in term of disconnection demand or generation with different capacities and duration.

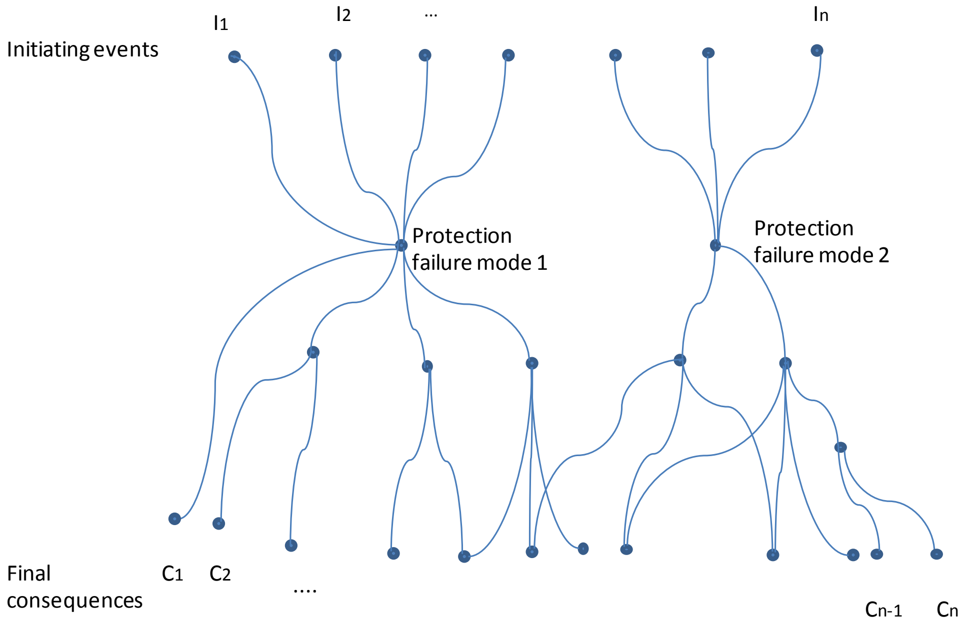

Figure 4.2. Diagram of scenario evolution of protection failure modes

One of the initiating events of the protection failure modes is the protection component failures. FMEA technique (section 3.2.1) can be used to examine the effect of each component failure on the protection system operation. The component failure may initiate failure to operate or unwanted operation. For example a spurious trip of a relay or circuit breaker causes unwanted operation of the protection.

Other causes of the protection failure modes can be found by analysed the working principle of the protection and power system quantity that can cause the protective relays to operate. Unwanted operation may occur if the power system produces the same abnormal quantity which recognized incorrectly by the relay as a fault. For example, in the case study of ROCOF protection in chapter 6, a large generation loss may produce a high rate of change of frequency which may be incorrectly sensed by the ROCOF relay as a loss of main condition and it may then send a trip command in error. The opposite could also be happen where the fault cannot be detected due to very low abnormal power system quantity such as a ROCOF protection fail to detected loss of main condition due to very low rate of change of frequency when the local demand balances with the DG output. Power system simulation can be used to find out the protection failure initiating events. For example the external faults positions and types that can trigger the unwanted operation.

Power system simulation is also a good way to reveal the possible scenarios of the system following protection failure modes. They include cascading effect, amount of generator or demand disconnection due to the cascading effect, etc.

For the simulation, the power system states may be varied in generation and demand, system inertia, generation mix, fault types, fault position, etc. Obviously, this will create a very exhaustive possible combination of scenarios. In order to limit the number of simulations, the varied elements can be grouped according to similarity of the effect to the system. For example, the occurrence a fault on the beginning of a line causes similar effects to the fault on the end of the line, hence it can be concluded that any of faults on the line can be represented by the both faults' effects and their simulation results. Moreover, continuous variables such as amount of generator output, demand, etc., also need to be divided into some intervals. For example demand can be grouped into some demand intervals; system inertia can be divided into group high, average and low inertia, etc.

4.6. Data and assumption

Historical data is the best source of data for the assessment; however it is not often available. The second source of data is generic data from literatures. Other sources of data are the protection simulation results and expert opinions. Sources of data have to be mentioned in the assessment report. The protection component failure rates may come from historical or generic literature data.

Risk assessment is often considered as an exhaustive work as it must consider every possible scenario of the assessed system. Although this is true, risk assessment of a power system protection can be simplified if the intended use of the assessment is permitted to do so using some assumptions. Generating some assumptions of the system behaviour will reduce the complexity of the scenario. For example in the case study distance protection with quadrature booster transformer (chapter 5), the scenario is simplified by assuming worst case scenario hence it avoids the need of power system stability simulation. Since the risk result is considered low, therefore the worst case scenario assumption can be accepted because the actual risk (without worst case assumption) should be relatively lower.

Futhermore, a more simple model can also be achieved by omitting the protection component failures. When comparing the risk of the same protection systems that work in different settings for example, the protection component failures can be excluded as the assessment focuses to the risk that is introduces by the setting choices. Protection component failures can be assumed to remain constant for any settings.

4.7. Risk assessment steps

The steps of conducting a power system protection risk assessment are:

a. Identification of the protection failure modes
b. Identification of the consequences of the protection failure modes
c. Identification of the initiating events of the failure modes
d. Construction of the risk model for probability calculation
e. Quantification of the occurrence probability of the failure modes
f. Quantification of the consequences of the protection failure modes
g. Validation of the risk model
h. Quantification of the risk of protection failure modes and the total risk
i. Sensitivity analysis
j. Implementation of the risk assessment result for decision making process.

The detail explanation of the steps is described in the following sections.

4.8. Identification of the protection failure modes

In general, failure modes of protection schemes can be divided into two main modes i.e. failure to operate and unwanted operation. Failure to operate mode is a condition when the protection fails to operate in the intended time for a specific fault in its protected zone. Unwanted operation mode is a condition where the protection operates when it should not. Failure to operate may involve complete failure to operate or operation longer than the intended duration.

Failure to operate modes of a protection can be found straightforwardly from operating modes which the protection is designed for. Some protection schemes may have one operating mode, hence create only one failure to operate mode. Others may have more than one operating mode hence create several failures to operate modes. For example, in chapter 7, the overcurrent relay has failure modes i.e. failure to operate instantaneously and complete failure to operate. As for distance protection case study in chapter 5, the failure to operate modes include failure to operate in zone 1, zone 2 and zone 3.

Unwanted operation modes can be categorised by their initiating event such as component failures, transient conditions which trigger the protection to operate or fault locations. In chapter 6 for example, the unwanted operation consists of two modes: due to large generation loss and due to nearby faults.

4.9. Identification of the consequences of the protection failure modes to the power system

Generally, failure to operate will cause remote backup protection to operate hence larger areas of the system have to be disconnected. This may cause unnecessary demand and generation disconnection. Similarly, unwanted operation may cause unnecessary disconnection of generator and demand. Depending on criticality of the demand/generation disconnection, cascading effect may occur following the disconnection. On distribution networks, the disconnection may not cause a cascading effect, but it may occur on transmission network. Therefore, power system simulation is needed to check the possibility of occurrence of the cascading effect.

The simulation of the cascading effect requires significant effort, as there are many possible scenarios and there are also limitations of the simulation software in accurately reflecting actual conditions. Moreover, validation of simulation results is not easy to obtain. Therefore, some assumptions which can simplify the analysis and the complexity of the simulation may be employed.

Some protection failure modes may have fatality consequences for people that present at the nearby of the electrical network. For example, in the event of ROCOF protection failure to operate due to non-detection zone as explained in chapter 6, islanding operation of DG can occur. The islanding operation is not equipped with sufficient earthing system hence it can bring danger to electrical personnel who work in the network. Therefore human fatality assessment is required to be carried out.

Another consequence that can occur is equipment damage. Example of this consequence can also be found on ROCOF protection case study in chapter 6. In the case study, if a ROCOF protection fails to operate during loss of mains condition, there is a chance that automatic recloser reconnects the DG in out-synchronism to the main system hence it can damage the DG.

4.10. Identification of the initiating events of the failure modes

The obvious initiating events of protection failure to operate are protection component failures. Any failures of a relay, circuit breaker, current transformer, voltage transformer, DC supply, communication channel or wiring that prevent them from doing their function can cause protection failure to operate. However, sometimes the component is equipped with backup; hence the failure only occurs if both main and backup components fail. Failures of protection component that trigger unwanted operation can occur on relays and circuit breakers.

Other initiating events of protection failure to operate can be identified from system scenarios. The following questions can assist in finding initiating events:

a. Does the protection setting cover the entire protected zone?

b. If the protection provides a backup, is it in well-coordinated with the main protection for any primary system condition?
c. Are there any circumstances that the relay cannot identify a fault due to primary system condition?

Similarly for protection unwanted operation:

a. Are there any circumstances that the primary system produces similar abnormal quantity which can be identified incorrectly by the relay as a fault?
b. If faults occur beyond the protected zone, can the relay fully distinguish them all and remain stable?

The potential initiating events need to be simulated in order to check whether it can cause the protection failure modes. Examples of the initiating events for different protection are as shown in table 4.1.

Table 4.1. Initiating event of protection failure modes

Protection Scheme	Failure mode	Initiating event
IDMT	Failure to operate	Component failures, resistive faults
	Unwanted operation	Component failures, inrush current
Distance Protection	Failure to operate in zone 1	Component failures, resistive faults
	Failure to operate in zone 2	Component failures, effect of remote infeed, resistive faults
	Failure to operate in zone 3	Component failures, effect of remote infeed, resistive faults
	Unwanted operation	Component failures, heavy loading, power swing.
ROCOF protection	Failure to operate	Component failures, local load in balance with DG output during loss of main.
	Unwanted operation	Component failures, transient in the network such as faults in the network, large generation/demand loss

High resistive faults can be another initiating event of protection failure to operate. However, this event is not included as the cause of protection failure modes because a dedicated protection is needed for this condition, according to references [1, 2].

4.11. Construction of the risk model for probability calculation

Risk models consist of two parts:

- Models for the occurrence of protection failure modes
- Models for the consequences of the protection failure modes

These models are constructed according to cause-effect sequences and both models are combined into a protection risk model. The models are used for probability calculation. How precisely the system should be modelled can be adjusted according the purpose, assumptions and scenarios of the assessment. It can be started with a simple model then if it is needed; it can be refined with more realistic and complex models.

In this thesis, the risk model is constructed using Bayesian Networks using GeNIe software from University of Pittsburgh [3]. Bayesian networks consist of a qualitative part in form of a directed acyclic graph to represent the model of the protection risk and a quantitative part that executes the probability calculation of risk. Other techniques can also be applied; however, Bayesian Networks have several advantages [4] which will be explained in section 4.13.

4.11.1. Models for the occurrence of failure modes

Models are started with the initiating events and then cause-effect relationships are modelled continuously until reaching the failure modes as shown in figure 4.3a. Each of the nodes consists of the node’s states and relative probability. The initiating event nodes require the probabilities relating to the occurrence of the events; while other nodes require conditional probabilities for given parent states. The risk model is influenced by available data. If probability data of the initiating events are unavailable, the model can be traced back to the causes of initiating events, as shown in figure 4.3b. For example, failure to operate of ROCOF protection has an initiating event of "loss of mains". If no statistical data of the occurrence probability of the loss of mains is available, the cause of loss of main, for example substation failure, can be employed as the parent nodes. Therefore, the loss of mains probability data can be replaced with substation failure data and a CPT which shows conditional probability of loss of mains for a given substation condition (failure or not failure).

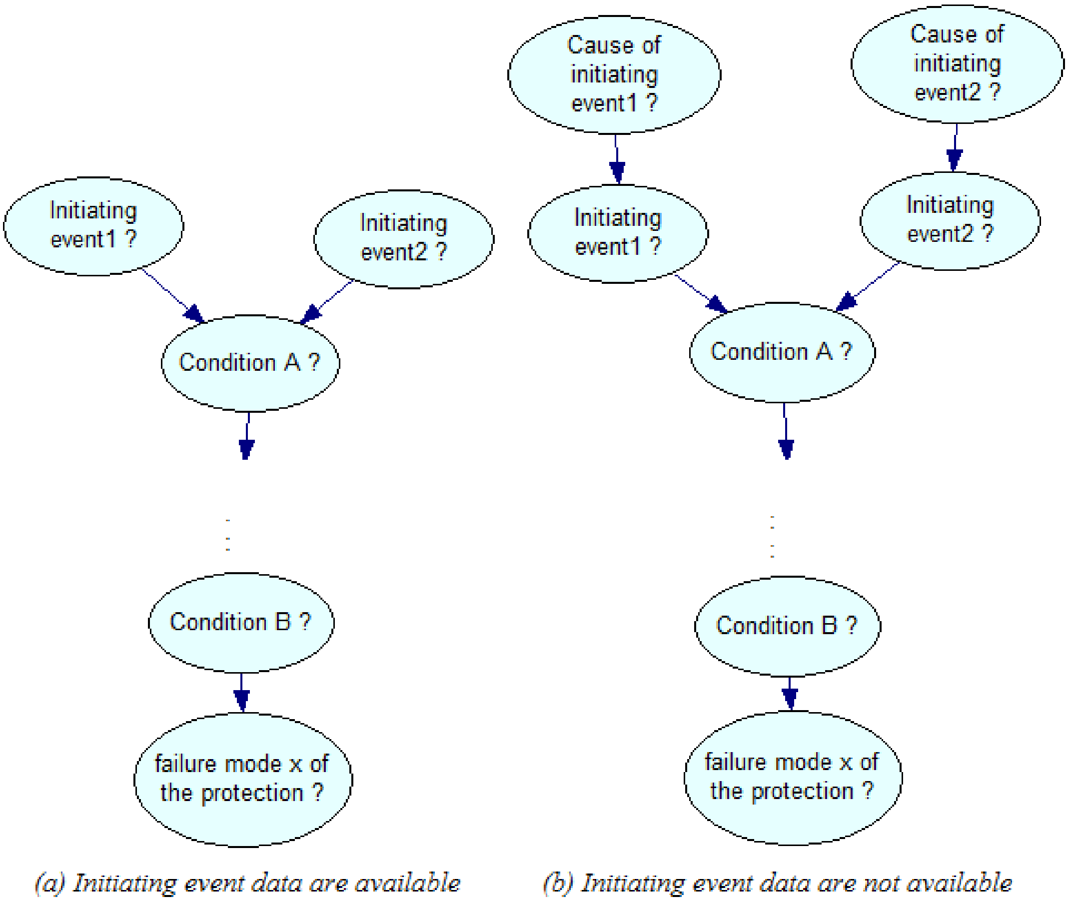

Figure 4.3. Model for the occurrence of failure mode x

4.11.2. Models for the consequences of failure modes

Once a failure mode of the protection takes place, the possible immediate effects are remote backup protection operation which may cause unnecessary disconnection of lines, demands, generation, etc. Based on scenarios and event sequences, models for the consequences of the failure modes can be constructed.

The effects of the protection failure modes is influenced by power system operating condition before the failure took place. For example, when a generator suffers unnecessary disconnection due to a protection failure mode, the cascading effect may occurs if the generator is supplying its maximum output. The cascading effect may not occur if the disconnection takes place when the generation is supplying less power. This condition can be modelled by employing multi-state representation of the generation output.

Figure 4.4 shows an example of a model for the consequences of failure modes. Following failure mode x of the protection, remote backup C may operate and it may cause disconnection of generator D. If the generator D is producing maximum output when the disconnection occurs, it may cause a reduction of power system frequency due to lack of generated power. This may trigger under frequency relay operation as shown in figure 4.4.

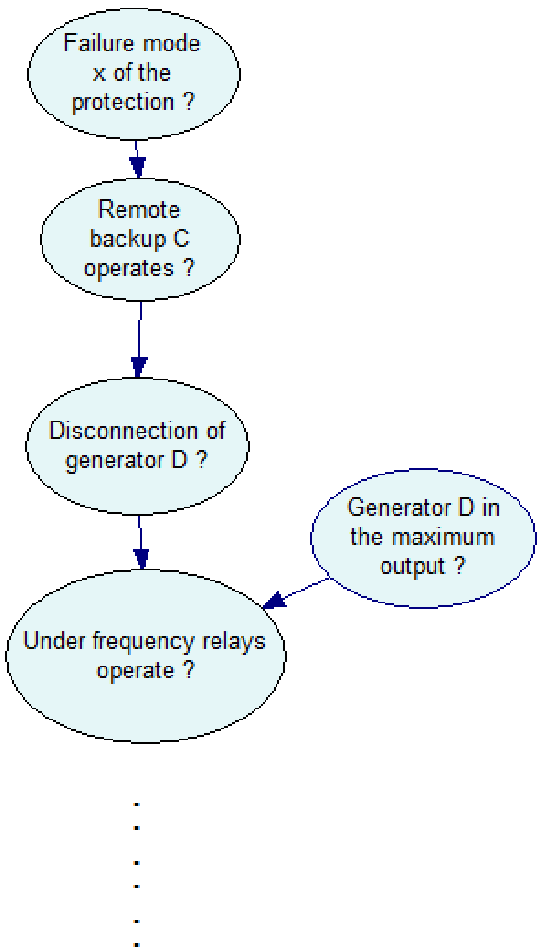

Figure 4.4. Model for the consequences of a protection failure mode

A combination of the two models (figure 4.3. and 4.4.) forms a risk model for a protection failure mode as shown in figure 4.5.

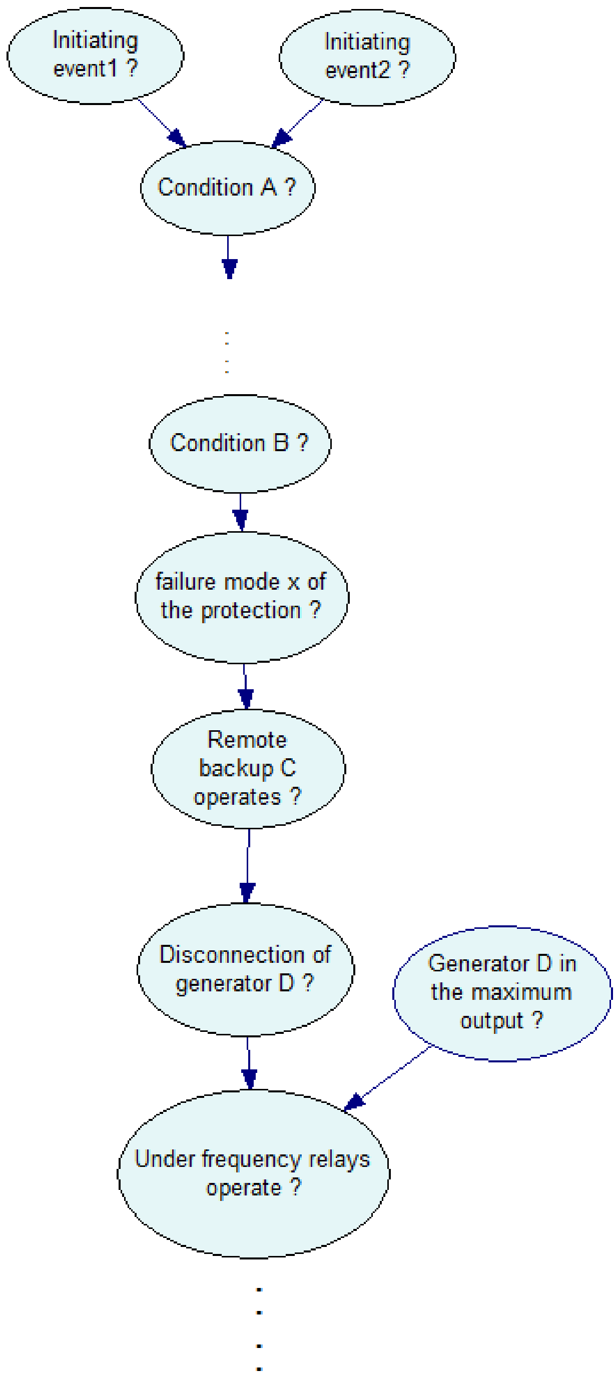

Figure 4.5. Risk model for a protection failure mode

4.12. Quantification of the occurrence probability of the failure modes

The choice of the probability calculation technique is based on the nature of the assessed system. Based on characteristics of the protection system and its protected system, four well-known probability calculation techniques have been compared in order to choose the best technique. The comparison is as follows.

In power system protection risk assessment, random variables often have more than two states. For example, protected systems may experience several types of fault: phase to ground, phase to phase, two phases to ground and three phase faults. Each of these faults has a different probability of occurrence and a different potential impact upon protection failure modes. If fault tree analysis is utilised, each fault type must be modelled as one random variable since it can only model 2 states for each variable (i.e. a fault type and no-fault state). Consequently, a number of risk models are needed to represent different combination of the variable states. Whereas using Bayesian Networks, a random variable can model any number of states. It certainly will simplify and reduce the number of risk models required.

Common causes of failure in protection system are not rare conditions. For example, a DC supply failure is a common cause of failure for relay and circuit breaker if they share the same DC supply. This condition can be modelled straightforwardly using Bayesian Networks, but it is not the case with Fault Tree. Moreover, Fault Tree analysis can only model deterministic gates (AND-OR gates) while Bayesian Networks provide unlimited conditional probability of cause-effect relationship. Therefore, fault trees are not the good technique for modelling the protection risk.

Although Markov analysis can model multi-state random variables and common causes of failure, it cannot handle large systems. As the protection components and other initiating events of protection failure modes are significant in number, employing Markov analysis will result in a massive Markov model which is difficult to be managed. Therefore, Markov analysis is impractical for power system protection risk assessment.

Monte Carlo simulation is a good candidate for the large number of components and initiating events of power system protection risk assessment. However, Monte Carlo simulation need detail data of statistical distribution (types and the related parameters) of random variable which is often not available. As for Bayesian Networks, the required data are in the form of simple probabilities which can be gathered from many sources, including expert opinions. Simple probabilities are a lot easier to define using limited information than detailed statistical distribution data, which requires extensive observation/information.

Based on these characteristics, Markov Analysis, Monte Carlo simulation and Fault Tree analysis have some disadvantages if they are applied for risk assessment of power system protection. On the other hand, Bayesian networks are able to fit with power system protection characteristics i.e. multi states, dependent variables, large-complex system and lack of statistical data. Therefore, the Bayesian Network is preferred to be used as the probability calculation technique. The occurrence probabilities of the protection failure modes can be calculated from their probability models using Bayesian Network software [3].

The data for Bayesian Network consist of :

- prior probabilities of protection component failures and other initiating events
- conditional probability tables (CPTs) which express the conditional probabilities of occurrence of descendant states for a given combination of parent node states. Data for CPTs are mostly gathered from simulation of the primary system for various system scenarios

The probabilities of protection components failures follow exponential distribution which is the common statistical distribution for electrical equipment in its useful life [5]. The probability of the protection component failure can be calculated as unreliability and unavailability as explained in section 4.3. Effect of a component failure upon protection failure modes is stated on a CPT.

4.13. Quantification of the consequences of the protection failure modes

There are two quantities need to be calculated for the failure mode consequence i.e. the likelihood and the magnitude of the consequence. All consequences which have economic value need to be calculated in terms of occurrence probabilities and costs. The consequences may also have social and political value [6] that are difficult to quantify and beyond the scope of this thesis. Occurrence probabilities of the consequences are calculated from the risk model (such as in figure 4.5.) using Bayesian Networks software. If the consequences bring hazard to human safety, it needs to be compared to a safety standards in order to identify whether the protection is safe to operate or not. Individual safety consequences will be explained later in this chapter.

An effective way to quantify the magnitude of consequences is using currency. Quantifying the consequence magnitude using power loss/unsupplied energy is considered ineffective because:

- The economic value of demand loss is different from generation loss although they have the same amount of power/energy. The economic value of the demand loss is related to the potential cost that the consumers may suffer from unexpected electricity outages, such as spoiled good or raw materials, loss of revenue and extra costs for loss of hours of work. The economic value of generation loss is mainly related to the cost of undelivered generation power/energy experienced by the generation owner.
- Sometime the consequences are not in form of demand or generation loss, but for example in form of equipment damage, then it is difficult to have a common measurement other than currency (financial cost)

The consequences that have economic value for example are generator disconnection, demand disconnection and damage to the equipment. Values of the consequences are determined by amount of capacity loss (MW) and duration of the disconnection (hour) as explained in the following sections.

4.13.1. Generation disconnection cost

Disconnection of a generator will incur three components of loss: profit loss suffered by the generator owner, generator shutdown-start-up cost and additional cost due to utilisation of expensive fast reserve generation.

The generator profit loss is calculated on the basis unsupplied energy and depends on type of generation (i.e. steam, nuclear, wind and etc.). Profit that the generator owner fails to receive is calculated as:

$$G_{profit} = P_{goutput} \times t_g \times C_{gprofit} \qquad (4.12)$$

Where:

G_{profit} = generator profit loss (currency)

$P_{goutput}$ = amount of undelivered generation power (MW)

t_g = duration of the generator disconnection (hour)

$C_{gprofit}$ = Profit per MWh generation of the corresponding generator type (currency/MWh)

In liberalisation of electricity markets, the generation profit varies widely due to variations in electricity price; therefore the value that should be taken is the recent year average. Other method to calculate generation profit/MWh is from the difference between the average electricity price and the generation levelized cost plus transmission (or distribution) charged. Levelized cost is the cost to generate per MWh of the electricity which is including capital cost, operating cost, maintenance cost over life time of the plant and based on assumed utilization rate of the plant [7]. For renewable generation, the revenue loss from selling renewable energy certificate (ROC) can also be included in the profit loss.

Generator shutdown-start-up cost, which is also known as cycling cost, is the cost that is incurred due to shut down and start-up of a generation unit. This cost is significant for thermal generation. Each shutdown-start-up of the power plant causes high thermal and pressure stress experienced by the boiler, turbine and other auxiliary components hence it increases the plant's failure rate. The higher failure rate results in higher capital and maintenance cost to replace the damage components [8]. The cycling cost consists of operation cost to start the plant and capital and maintenance cost of the damage components. Shutdown duration influences the shutdown-start-up cost. Based on shut-down durations, there are three types of start-up i.e. cold, warm and hot starts. For coal generation, a shutdown duration of more than 40 hours results in a cold start. Between 12 to 40 hours duration leads to a warm start and less than 12 hours duration is a hot start. The cost is proportional to the shut-down duration as shown in table 4.2.

Table 4.2. Median shutdown-start-up cost of fossil fuel generation [8]

Unit type	Large Coal	Gas-CCGT
Hot start cost, $/MW cap	59	35
Warm start cost, $/MW cap	65	55
Cold start cost, $/MW cap	105	79
Warm start duration, hours	12-40	5-40

Generation shutdown-start-up cost G_{cyc} is calculated as follows

$$G_{cyc} = P_{gcap} \times C_{gcyc} \tag{4.13}$$

Where

P_{gcap} = generator capacity (MW)

C_{gcyc} = shutdown-start-up cost (currency/MW capacity)

Utilisation of fast reserve generation by transmission network operator to replace the loss of supply incurs utilisation cost. In GB power system, the utilisation cost of fast reserve generation is based on monthly tender submission to National Grid. Table 4.3 shows monthly average utilisation cost for year 2013. The 2013 average fast reserve utilisation cost is £143.28/MWh, which is more expensive than the average electricity price £120.41/MWh [9]. Therefore there is £22.87/MWh deficiency due to utilisation of fast reserve generation. The additional cost of utilisation of fast reserve generation $G_{reserve}$ is calculated as shown in equation (4.14).

$$G_{reserve} = P_{goutput} \times t_g \times dC_{greserve} \tag{4.14}$$

$P_{goutput}$ = amount of undelivered generation power (MW)

t_g = duration of the generator disconnection (hour)

$dC_{greserve}$ = additional cost for utilization of fast reserve generation (currency/MWh)

Table 4.3. Utilisation fast reserve generation price, National Grid market information 2013 [10]

Month	Total cost(£)	Quantity (MWh)	cost(£/MWh)
January	4320000	30020	143.904064
February	3890000	26470	146.9588213
March	2860000	19590	145.9928535
April	2730000	19200	142.1875000
May	3190000	22910	139.2405063
June	2460000	17200	143.0232558
July	1990000	13900	143.1654676
August	2340000	16520	141.6464891
September	2420000	16910	143.1105855
October	1670000	11630	143.5941531
November	3040000	21280	142.8571429
December	1610000	11210	143.6217663
total average 2013			143.2752171

Therefore, total generator disconnection cost is:

$$C_{gen} = G_{profit} + G_{cyc} + G_{reserve}$$

$$C_{gen} = (P_{goutput} \times t_g \times C_{gprofit}) + (P_{gcap} \times C_{gcyc}) + (P_{goutput} \times t_g \times dC_{greserve}) \qquad (4.15)$$

4.13.2. Demand disconnection cost

Demand disconnection cost is based on a model developed in [11] which consists of customer interruption cost and unsupplied energy cost. The customers are divided into five common groups: residential, agricultural, industry, public and commercial sector. The interruption cost for each sector is calculated based on survey of consumer's losses due to power interruption for different durations (one second to 8 hours). To obtain the cost of interruption and unsupplied energy, the costs of each group are processed into a linear regression as shown in figure 4.6 The slope of the linear regression represents the cost unsupplied energy (currency/MWh) and the intersection to y axis represents cost of interruption (currency/MW) [11]. The cumulative cost of all sectors is the weighted average based on each group percentage. The cumulative cost is also processed into a linear regression to obtain interruption cost (currency/MW) and unsupplied energy cost (currency/MWh).

The total demand disconnection cost C_{demand} is calculated as follows:

$$C_{demand} = C_f \times P_{demand} + C_u \times P_{demand} \times t_d \tag{4.16}$$

Where:

C_f = demand interruption cost (currency/MW)

P_{demand} = unsupplied demand (MW)

C_u = unsupplied energy cost (currency/MWh)

t_d = duration of demand disconnection (hour)

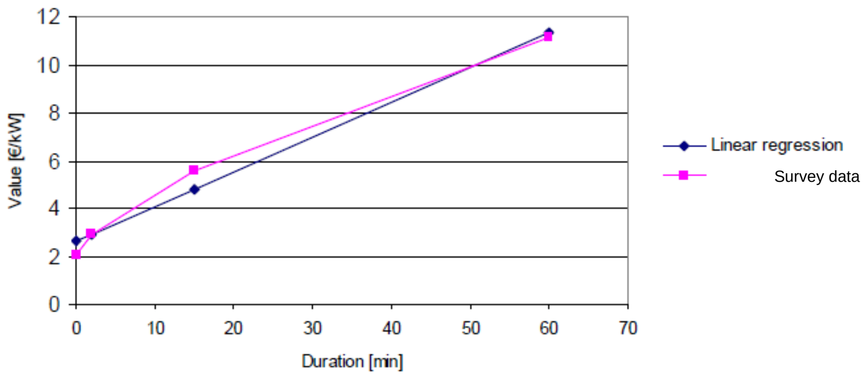

Figure 4.6. Cost of demand disconnection, from survey and linear regression [11]

In the UK, demand disconnection cost is expressed in term of Value of Load Loss (VOLL). VOLL represents value of electricity for the user in term of security of the electricity supply[12]. Domestic, small and medium sized businesses and industrial-commercial electrical consumers are surveyed for their value of electricity outage for different length, season, days of the week and time of the day. The results give

VOLL for each consumer group, and then, they are averaged based on the percentage of each consumer group. The recommended VOLL for all customer is £16,940/MWh [12]. If using this VOLL, then demand disconnection cost is only calculated based on duration of the disconnection without considering the frequency of disconnection. As consequence, two one-hour disconnections will incur the same cost as a two hour disconnection, which is not correct as the former will be more costly [13]. Therefore, if the available data allow demand interruption cost and unsupplied energy cost to be calculated, then these two costs should be used, as they represent the more realistic costs.

4.13.3. Equipment damage cost

The cost of equipment damage is calculated as an asset loss which value is based on *book value* of the equipment when the damage occurs. Book value is calculated as:

$$B = I - D.t_e \tag{4.17}$$

Where

B = book value (currency)

I = investment cost (currency)

D = annual depreciation charge (currency/year)

t_e = duration of the equipment has been utilised (year)

The investment cost is total cost of the equipment, including capital cost, tax, installation cost and site preparation. Depreciation is a decrease in value of the equipment. Depreciation is calculated using straight-line method as in equation (4.18) which is the most common way to calculate depreciation [14].

$$D = (I - R)dr = \frac{I - R}{life} \tag{4.18}$$

Where

R = residual value of the equipment at the end of its life (currency)

dr = depreciation rate = $\frac{1}{life}$ (%)

$life$ = predicted useful life of the equipment (year)

If the damage occurs on generation equipment hence it discontinues the generating process. The expected profit loss for a predicted duration (i.e. until a replacement ready to operate) has to be calculated as another consequences of equipment damage. Equation (4.12) can be used to calculate the profit loss.

4.13.4. Individual safety

Individual safety needs to be concerned if the protection failure modes cause a hazardous condition for people in vicinity of the primary system. For example in chapter 6, failure of ROCOF protection to detect loss of main condition due to the balance of local demand to DG output causes undetected islanding operation of a DG. The islanding operation is not permissible because the islanding network does not have earthing system hence it can be hazardous for workers in vicinity of the network.

The probability of a person to be killed due to the hazardous condition must be very low otherwise the protection scheme cannot be applied. The UK Health and Safety Executive (HSE), provides a safety criteria for individual or worker in [15]. The criteria are illustrated in Figure. 4.7. and can be used to check whether the anticipated risk of human fatality due to protection failure mode is acceptable. The numbers in figure 4.7 are the annual probabilities of a worker being killed.

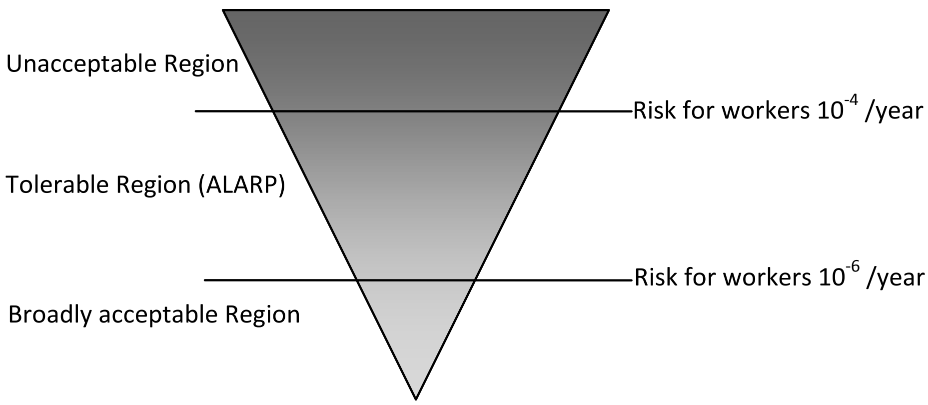

Figure 4.7. Human fatality risk criteria [15]

If the risk of human fatality falls into the unacceptable region, clearly the protection scheme is not safe to operate. Therefore, it will be rejected and the risk assessment is terminated. If the risk falls into broadly acceptable region ($P \leq 10^{-6}$) then the fatality risk is insignificant then human fatality risk element can be eliminated from the overall risk. An additional analysis is needed should the risk fall into ALARP (As Low As Reasonably Practicable) region. The analysis should attempt to reduce the risk into acceptable region using available options such as installation of additional equipment which will incur an additional cost. This cost is added to the total cost of the protection system. The cost of a protection candidate will influence in decision making.

4.14. Validation of the risk model

Model validation is an important step as it examines whether the models that have been made represents the correct condition. The method of model validation, which is based on the validation method reported in [16] is as follows:

a. A slight increase/decrease in probability of each parent node should cause relative increase/decrease in posterior probability of the descendant node.
b. If all initiating event probabilities are increased, the occurrence probability of the final consequences is also increase in a magnitude which is not smaller than when only one initiating event is increased.

4.15. Quantification of the risk of protection failure modes and the total risk

Risk is calculated as a product of the probability of the failure consequence and its cost in currency. The risk result is expressed in currency per a mission time, for example £/year, €/day and etc. If the probability of generator disconnection due to failure mode *i* is multiplied to the equation of generator disconnection cost (4.8), the result is the risk of generator disconnection due to a protection failure mode *i* as shown in equation (4.19)

$$R_{gen-i} = C_{gen} \times F_{g-i} = (P_{goutput-i} \times t_{g-i} \times F_{g-i} \times C_{gprofit}) + (P_{gcap} \times C_{gcyc} \times F_{g-i}) + (P_{goutput-i} \times t_{g-i} \times F_{g-i} \times dC_{greserve})$$

$$R_{gen-i} = (P_{goutput-i} \times d_{g-i} \times C_{gprofit}) + (P_{gcap} \times C_{gcyc} \times F_{g-i}) + (P_{goutput-i} \times d_{g-i} \times dC_{greserve}) \quad (4.19)$$

Where:

F_{g-i} is probability of the occurrence of the generator disconnection due to the protection failure mode i.

d_{g-i} is the expected generator disconnection duration due to the protection failure mode i (hours/year or hours/day) = $t_{g-i} \times F_{g-i}$

Similarly for demand disconnection cost, the risk of demand disconnection cost due to a protection failure mode i is shown in equation (4.20).

$$R_{demand-i} = (C_f \times P_{demand} \times F_{demand-i}) + (C_u \times P_{demand-i} \times d_{demand-i}) \quad (4.20)$$

Where

$F_{demand-i}$ is probability of the occurrence of the demand disconnection due to the protection failure mode i.

$d_{demand-i}$ is the expected demand disconnection duration due to failure mode i (hours/year or hours/day) = $t_{d-i} \times F_{demand-i}$

Equally, equipment damage risk is as shown in equation (4.21).

$$R_{dam-i} = (F_{dam-i} \times B) + \ (P_{goutave} \times d_{gre-i} \times C_{gprofit}) \quad (4.21)$$

Where

F_{dam-i} is probability of occurrence of the equipment damage due to failure mode i,

$P_{goutave}$ is average output of the generator before the damage occurs (MW) due to failure mode i

d_{gre-i} is the expected duration of the generator repair or replacement (hour).

The risk of a failure mode i is a sum of the risk from generator and demand disconnection and equipment damage as shown in equation (4.22).

$$R_i = R_{gen-i} + R_{demand-i} + R_{dam-i} \tag{4.22}$$

Where

R_{gen-i} is risk from generator disconnection due to failure mode i

$R_{demand-i}$ is risk from demand disconnection due to failure mode i

R_{dam-i} is risk from equipment damage due to failure mode i

The total risk of a protection scheme is sum of the risk due to failure modes:

$$R_T = \sum_{i}^{n} R_i \tag{4.23}$$

Where

R_T = total risk of the protection scheme

R_i = risk of protection failure mode i

n = number of the protection scheme failure modes

The total risk will be used as parameter for decision making of power system protection, while also considering the costs of the protection system.

4.16. Sensitivity analysis

After a risk assessment has been conducted, sensitivity analysis is needed since there are always uncertainties in some probability data. Sensitivity analysis provides additional validation of the risk results [17]. The sensitivity analysis finds the effects of changes in the probability data upon the risk results. It is usually carried out for one variable at a time while keeping other variables constant. The probability of the variable is varied for lower and higher probabilities than the base case. The sensitivity analysis shows the effect of different probabilities of the event to the risk and it can also show which initiating events have significant impact to the risk results.

4.17. Implementation of the risk assessment framework for decision making process

Risk assessment results provide decision support for implementation of power system protection schemes. All alternatives of the protection schemes/setting can be ranked according their calculated risk. Sensitivity analysis results should also become important consideration in measuring uncertainty of the base case results. Several case studies are presented to illustrate the risk based decision making i.e.:

- Evaluation of an existing protection scheme following changes in primary system condition (example in chapter 5)
- Finding the optimum setting of a protection scheme (example in chapter 6)
- Selection of the best protection scheme for a given protected system (example in chapter 7)

If the condition of a protected system changes, such as due to installation of equipment with new technology, the existing protection performance may deteriorate. Risk assessment can be utilised to reveal whether the protection still works as intended or to ascertain whether it suffers significant deterioration. If the risk result shows unacceptable increase of the risk, the existing protection has to be modified or replaced. In order to choose a new protection scheme to replace the existing one, risk assessment can be utilised in the protection selection process. Before selection process is started, risk assessment can be used to find the optimum setting of each protection candidate. Then the risk of each protection scheme in their optimum setting can be compared in order to choose the best protection scheme. The flowchart of this process is shown in figure 4.8.

The case studies in chapter 5, 6 and 7 illustrate implementation of the risk assessment according to the proposed framework. For probability quantification of the case studies, Bayesian Network software is required. There are several Bayesian Network software packages that can be used. One of them is GeNIe which is developed by Decision System Laboratory of University of Pittsburgh [3]. GeNIe software is employed for the case studies.

GeNIe has a graphical editor to create and modify risk models. From the model, the node states can be defined and the probability data can be assigned. The probability calculation of the model is relatively fast i.e. less than a second for the models in this thesis. The software also has the capability to find the nodes which have significant influence to certain consequences of the failure mode. Therefore this facility will assist in conducting sensitivity analysis as describe in section 4.16.

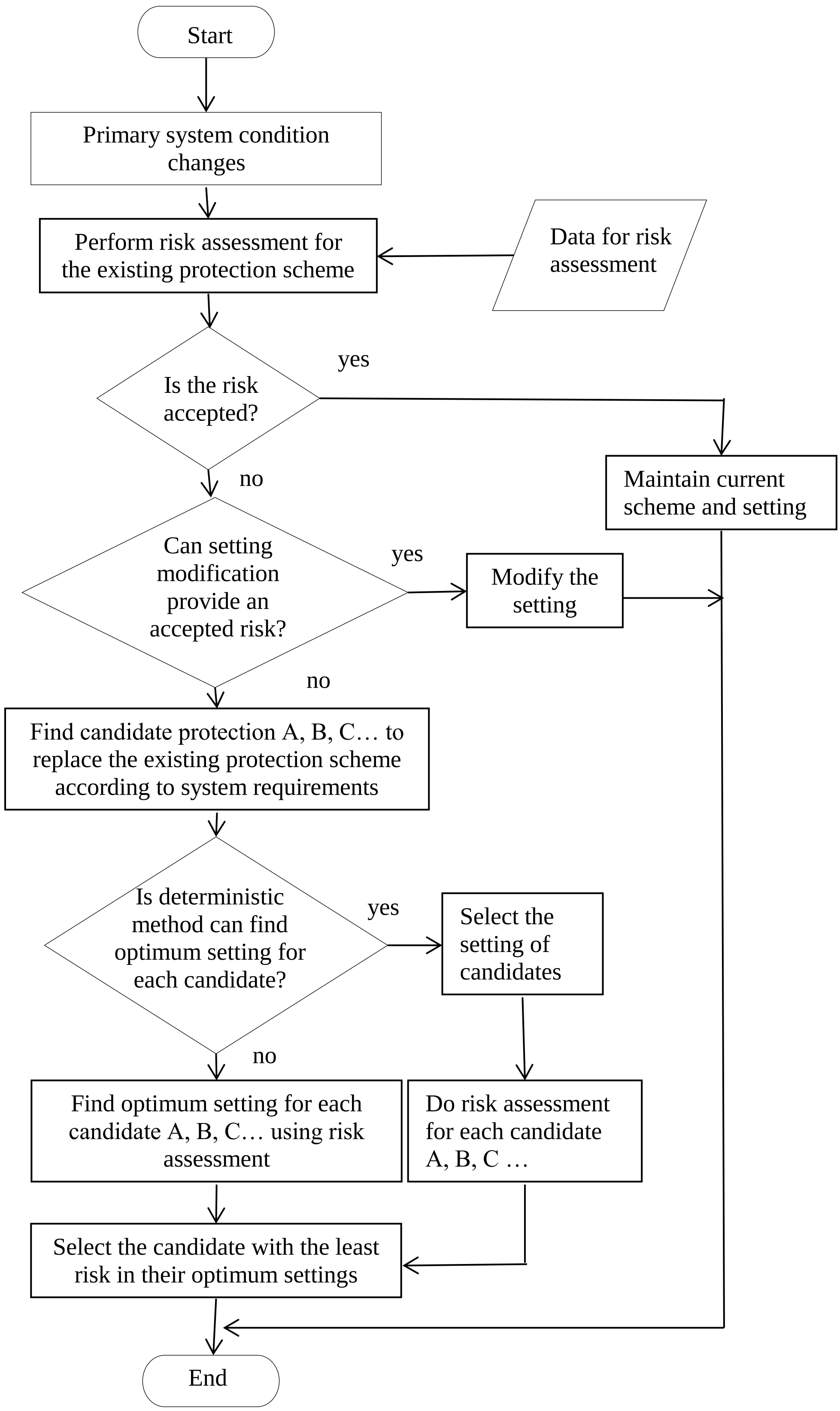

Figure 4.8. Flowchart of risk assessment based decision making process for selecting a protection scheme following primary system change

4.18. Conclusion

A dedicated risk assessment framework for power system protection has been developed. The framework, which uses Bayesian Networks for probability modelling and calculation, has an important contribution in any intended use of power system protection risk assessment. Quantification of the magnitude of protection failure consequences has been developed which includes human fatality and economic values of equipment damage and generation and demand loss. A guidance to simplify the risk model has been also introduced which is based on the intended use of the assessment through the underlying assumptions and scenarios. Three case studies to illustrate the framework in different intended use and modelling levels are presented in chapter 5, 6 and 7.

4.19. References for Chapter 4

[1] B. M. Aucoin and R. H. Jones, "High impedance fault detection implementation issues," *Power Delivery, IEEE Transactions on,* vol. 11, pp. 139-148, 1996.

[2] C. L. Benner and B. D. Russell, "Practical high-impedance fault detection on distribution feeders," *Industry Applications, IEEE Transactions on,* vol. 33, pp. 635-640, 1997.

[3] Decision System Laboratory University of Pittsburgh. (2010, 27 July). *GeNIe 2.0*. Available: http://genie.sis.pitt.edu/

[4] A. Bobbio, L. Portinale, M. Minichino, and E. Ciancamerla, "Improving the Analysis of Dependable Systems by Mapping Fault Tree into Bayesian Networks," *Reliability Engineering and Safety,* vol. 71, pp. 249 - 260, 2001.

[5] IEEE-SA, "IEEE std 493-2007 Recomendation Practice for the Design of Reliable Industrial and Commercial Power Systems," ed. New York: IEEE, 2007.

[6] H. Brayley, M. A. Redfern, and Z. Q. Bo, "The Public Perception of Power Blackouts," in *Transmission and Distribution Conference and Exhibition: Asia and Pacific, 2005 IEEE/PES*, 2005, pp. 1-5.

[7] U.S-Energy-Information-Administration, "Annual Energy Outlook 2014, with Projection to 2040," EIA, Washington DC2014.

[8] N. Kumar, P. Besuner, S. Lefton, D. Agan, and D. Hilleman, "Power Plant Cycling Costs," NREL, Colorado2012.

[9] I. MacLeay. (2014, March 2014). Domestic energy bills in 2013: The impact of variable consumption. *Energy trends statistical March*

[10] National_Grid, "Fast Reserve, Market Information for Tenders for March 2013 - March 2014," National grid, London2013-2014.

[11] K. Kivikko, A. Mäkinen, P. Järventausta, J. Lassila, S. Viljainen, and J. Partanen, "Methods for advanced compilation of interruption statistics to cater the renewing regulation," *Proceedings of NORDAC 2004*, 2004.

[12] London-Economics, "The Value of Lost Load (VoLL) for Electricity in Great Britain. Final report for OFGEM and DECC," London Economics, London2013.

[13] Task-Force-38.06.01, "Methods to Consider Customer Interruption Costs in Power System Analysis," Cigre, Paris2001.

[14] C. S. Park, *Fundamentals of engineering economics*: Prentice Hall, 2004.

[15] COMAH. (06/02/2013). *Risk analyses or 'predictive' aspects of comah safety reports guidance for explosives sites*. Available: http://www.hse.gov.uk/comah/assessexplosives/step5.htm

[16] D. Zhang, X. P. Yan, Z. L. Yang, A. Wall, and J. Wang, "Incorporation of formal safety assessment and Bayesian network in navigational risk estimation of the Yangtze River," *Reliability Engineering & System Safety*, vol. 118, pp. 93-105, 10// 2013.

[17] R. R. Fullwood, *Probabilistic safety assessment in the chemical and nuclear industries*, 2 ed. Woburn: Butterworth-Heinemann, 2000.

Chapter 5. Case Study: Distance Protection for Transmission with Quadrature Booster Transformer

This case study is based on a specific protection issue faced by National Grid [1]. The risk assessment framework is used to evaluate existing distance protection after a change in the primary system due to installation of a quadrature booster transformer. The result will be used to justify whether the distance protection can be maintained or needs to be changed/modified. The case study also shows that modelling level of the assessment can be simplified according to the purpose of the assessment.

5.1. Introduction

A Quadrature Booster transformer (QB) is applied in transmission system to control the magnitude and direction of active power flows in transmission lines. This control is achieved by introducing a phase shift in the voltage angle across the transmission line [2]. A QB operates in three states, boost, buck and nominal states, with a number of taps for each boost and buck state. The nominal state is a condition where no phase shift is introduced to the transmission line. However, the QB may have negative effect for distance protection on the transmission line as it changes line impedance seen by the protection relay. This may cause under reach of the distance protection for zone 2 and zone 3 operation [1].

Zone 2 and zone 3 operation failure of the distance protection may not have significant occurrence probability because the existence of failure in zone 2 or zone 3 requires failures of all local protections (and also zone 2 remote backup for zone 3 operation failure). The local protections which consist of a unit protection, a distance protection and an Inverse Definite Minimum Time (IDMT) earth fault protection provide multi-layered protection [3]. However as the line where the QB is installed, i.e. 400KV feeder, is a very important feeder, failure to clear the fault may lead to instability if the fault clearing time is longer than the critical clearing time. A critical clearing time is the maximum duration which a disturbance can remain on the system without losing system stability. Therefore, the risk of distance protection failure to operate due to QB operation needs to be assessed. The risk assessment result can be used to decide whether the existing distance protection can be maintained or needs to be replaced or modified with other protection/characteristics.

5.2. Distance protection for transmission line with quadrature booster transformer

In GB power system, 400 kV transmission lines with length more than 10 km are equipped with two main protections, one local backup and two remote backups [3]. The main protections consist of one unit protection and one distance protection with permissive tripping. Permissive tripping is a scheme for a faster operation of distance protection for faults beyond zone 1 (>80% of the line length) by sending a trip command from a remote end relay to initiate a breaker trip. The trip command is verified with the detected fault by the local distance relay. Both have independent protection components and independent trip coil in order to avoid common failure but they share a circuit breaker. The circuit breaker is equipped with circuit breaker failure protection in order to reduce the possibility of fault clearing failures by the circuit breaker. Both of the main protections work with one-out-of-two trip logic i.e. tripping can take place if at least one protection sends a tripping command. The local backup is provided by IDMT protection for earth faults. The IDMT protection also has independent protection components and a trip coil, but shares a circuit breaker with the main protections. The remote backups are provided by 2 distance protections in zone 2 and zone 3 operating time [3].

A QB is applied for the case study's power system shown in figure 5.1 [4]. Data for the power system and its protection can be found in appendix A. The system consists of three power plants, a QB and five demands. In each breaker symbol which is labelled with Pxx, there are two main protection schemes i.e. differential protection and distance protection, and a local back up i.e. IDMT protection for earth faults. For example in P2a position, there are differential protection P2a, Distance protection P2a and IDMT protection P2a.

This case study will focus on the distance protection at position P1a. Zones of distance protection P1a are shown in figure 5.1. Distance protection P1a will work normally for faults on line WBUR-HIGM, but may suffer under reach for fault beyond the QB due to QB operation i.e. faults on line HIGM-RATS, RATS-WILE and RATS-STAY for zone 2 and zone 3 operations. As for distance protection P2a, it will not be affected by the QB because its position on line HIGM-RATS is after the QB. The risk assessment case is based on setting of distance protection P1a in table 5.1.

Since the intended use of a QB is to control direction and amount of power flow after an occurrence of fault [5], the corrective action is done using 16 tap-changers (boost1 to boost8 and buck1 to buck8) [4]. The tap switching is tele-operated by operator from control centre in substation [5]. During normal condition, the QB is usually in nominal state.

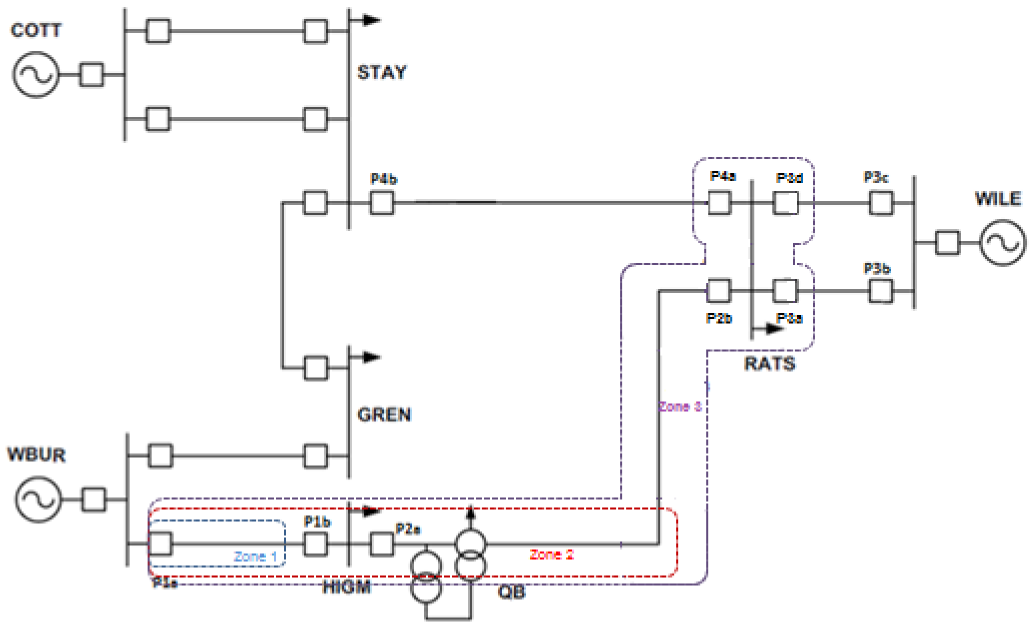

Figure 5.1. The power system with Quadrature Booster transformer (QB) [4]

Table 5.1. Setting of the distance protection P1a [4]

Protection zone	Reach (Ω)	Maximum Reach (QB bypass)
Zone 1	0.994	80% of line WBUR-HIGM
Zone 2	3.918	50% of line HIGM-RATS
Zone 3	7.663	16% of line RATS-WILE 6% of line RATS-STAY

The extent of protection under reach is influenced by the QB tap position and type of fault. Smaller tap position number causes more under reach and for the same tap position number; buck state produces more under reach than boost state. The reaches consecutively decrease for three phase (LLL) faults, line to ground (LG) faults and line to line (LL) faults. The reaches of distance protection P1a for LL fault are shown in figure 5.2 for QB in boost tap and figure 5.3 for buck tap. The graphs show the reaches are for faults on 0%, 30%, 50%, 70% and 100% of line HIGM-RATS. From the figures can be seen that buck state has less reach than boost state and tap buck1 produces the worst condition.

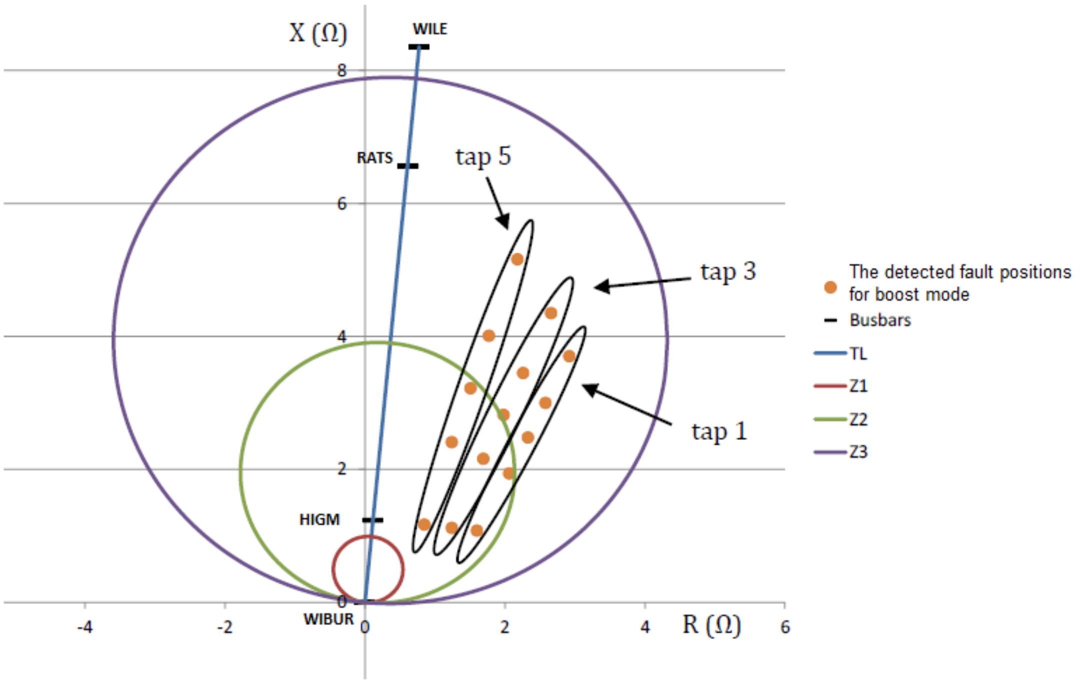

Figure 5.2. Under-reach of distance protection for boost state of the QB [4]

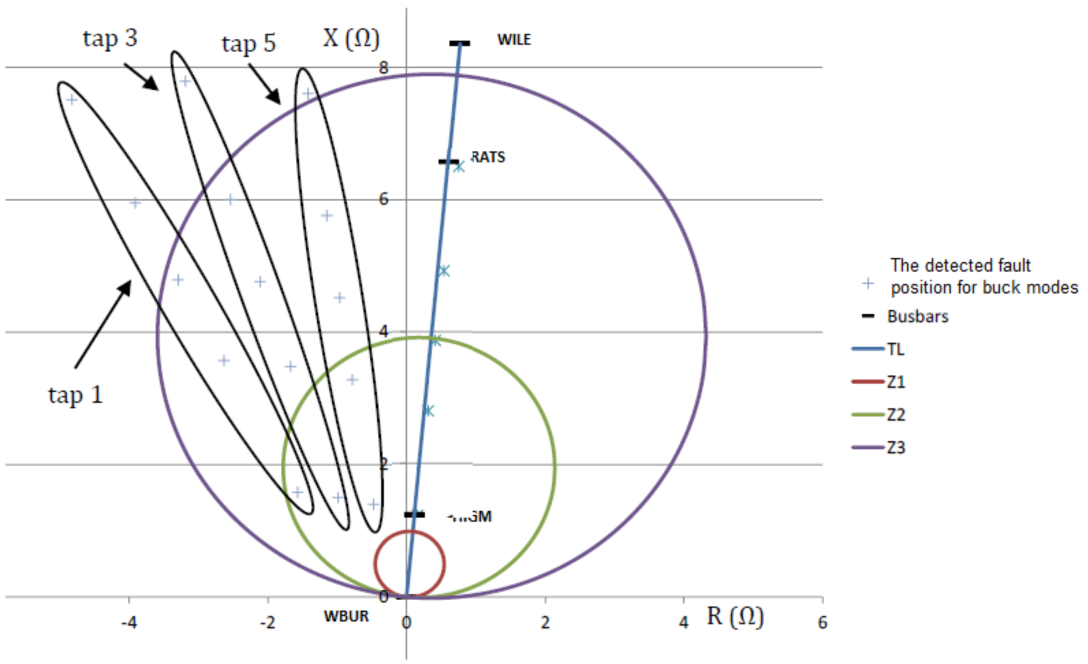

Figure 5.3. Under-reach of distance protection for buck state of QB [4]

5.3. Assumption and data in the study

Some assumptions are applied for this assessment in order to simplify the work and make the work possible to carry on. The assumptions are:

- Measurement errors of instrument transformers are negligible.
- Line parameters are assumed accurate.
- Unwanted operation due to high load current is negligible.
- The risk assessment only assesses additional risk introduced by QB hence component failures of the assessed protection will not be included.
- The intended operation of the QB is as a post fault correction tool, therefore the operational probability of each QB tap is based on unavailability of the particular generations
- Disconnection of the faulted section up to zone 2 operating time is assumed to be able to maintain system stability, however disconnection longer than zone 2 operating time will cause instability and may lead to blackout. This pessimistic assumption is chosen for the first stage of the risk assessment. If the risk results from this first stage are acceptable then the actual risk will also be acceptable since it should be less than these pessimistic assumption results. If the first stage risk is unacceptable then the more realistic assessment condition is needed. The pessimistic assumption is carried out in order to avoid a need for power system stability simulation.

The last two assumptions will limit the usage of assessment result i.e. only for evaluation of the additional risk of distance protection that introduced by QB operation. Although the assessment result will be pessimistic it certainly reduces the complexity of scenarios and models of the assessed system. Therefore the assessment can be carried out efficiently.

Data for probability quantification are collected from literatures and results of power system simulation using RTDS software [6]. Simulation of the system in figure 5.1 is carried out using an existing RTDS programme which is developed in previous research [4] at University of Strathclyde.

5.4. Protection failure modes and their consequences

There are four failure modes of the distance protection i.e. failure to operate in zone 1, zone 2 and zone 3 times and unwanted operation. The initiating events and consequences of the failure modes are shown in table 5.2.

Table 5.2. Initiating events and consequences of the distance protection P1a failure modes

Failure modes	Initiating events	Consequences
Failure to operate in zone 1 time	Protection component failures	If other main and local backup protections also fail, then remote backup will operate hence generator WBUR will be disconnected
Failure to operate in zone 2 time	Under-reach for certain tap of the QB	Distance protection P1a will operate in zone 3 time. This can cause stability problem
Failure to operate in zone 3 time	Under-reach for certain tap of the QB	Power system instability
Unwanted operation	Relay or circuit breaker spurious trip	Line WBUR-HIGM will be trip

Failure to operate in zone 1 time and unwanted operation are caused by distance protection component failures. These failure modes are not an effect of employing the QB. In order to simplify the assessment, this case study only assesses the additional risk introduced by QB operation. The failure modes which have initiating event from protection component failures will not be included in the assessment. Therefore the remaining failure modes that will be analysed are failure to operate in zone 2 and 3. Hence the risk assessment result will show additional risk introduced by installation of the QB to the conventional distance protection operation.

5.5. Modelling the risk of protection failure modes

Based on the initiating events and consequences of the protection failure modes, models for failure mode risk assessment are constructed.

5.5.1. Model for failure to operate in zone 2 time

The distance protection P1a requires working in zone 2 time if all local protections at P2a (a unit protection, a distance protection and an IDMT protection) fail to operate [3]. The unit protection only works if both unit protections at each end of the line function correctly and communication between them is operational. The distance protection will function if all its components function correctly and similarly for the IDMT for earth faults. Applying these conditions, the Bayesian network model for local protection (P2a) failure is shown in figure 5.4. The protections will fail to operate if one of the components does not function, such as VT, CT, relay, DC supply, breaker or wiring failure. The nodes which have the same colour, contribute to the failure of the associated protection system, for example the IDMT protection may fail if any of its components which are in yellow, is not functional. For communication and circuit breaker (CB), which may be shared between multiple protection systems, their failure can cause the failure of the connected protection systems.

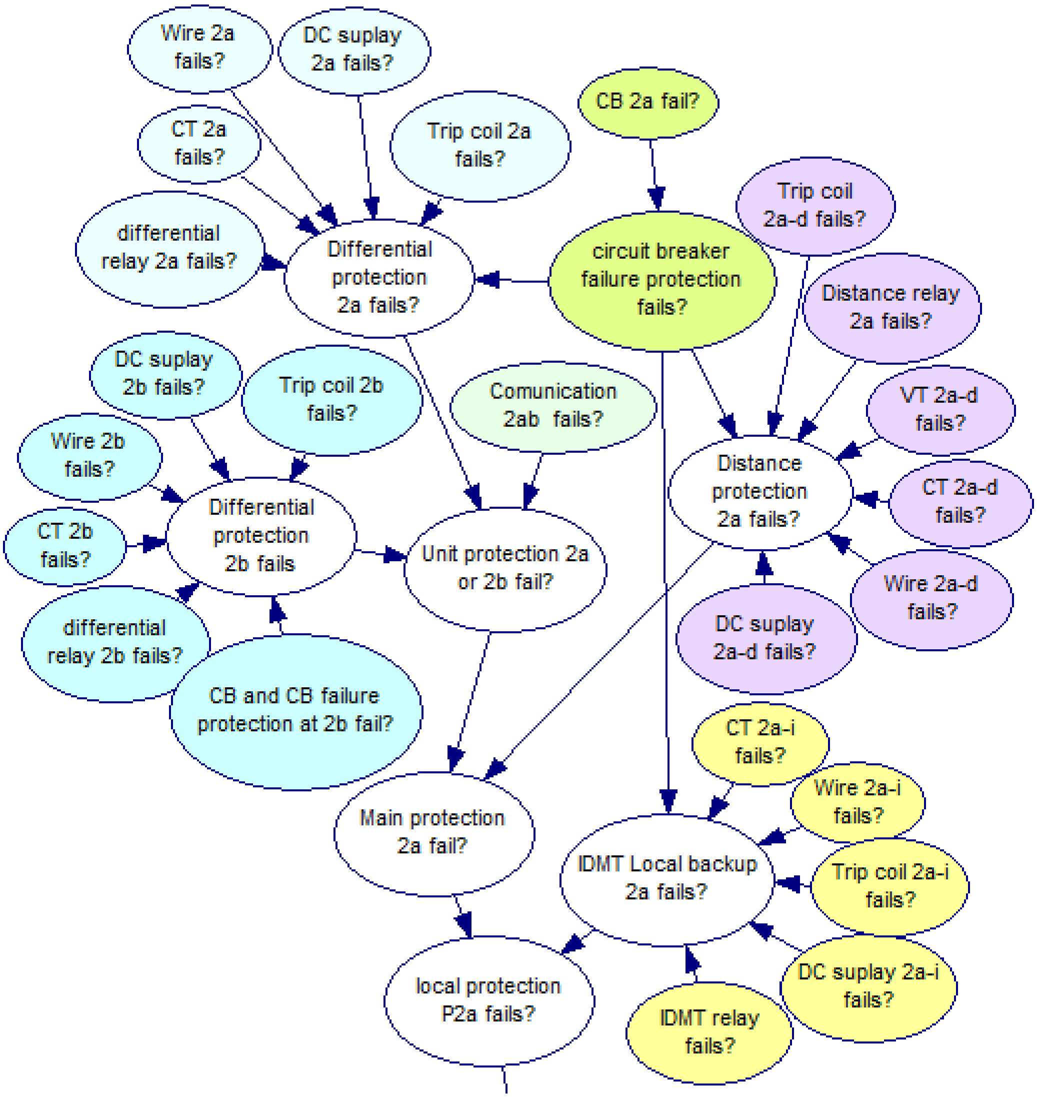

Figure 5.4. Model for local protection P2a of transmission line HIGM-RATS fail

The relationships between parent nodes which affect the descendant nodes are not shown in the model. The relationships are assigned in the conditional probability tables (CPT) of the descendant nodes. For example the CPT of node 'Main protection 2a fail?' is shown in table 5.3. The parent node 'Unit protection 2a or 2b fails?' has two states (fail and not fail) which are shown at the next columns in the same row of the cell 'Unit protection 2a or 2b fails?'. The parent node 'Distance protection 2a fails?' also have two states, fail – not fail. The states of the both node 'Distance protection 2a fails?' and the node 'Unit protection 2a or 2b fails?' are combined to cause the state of node 'Main protection 2a fail?'. The state of node 'Main protection 2a fail?' i.e. Fail and Not fail are shown at the last two rows of the table. From table 5.3. it can be seen that the main protection 2a will fail if only both of the distance and the unit protection fail, which is similar with AND gate for fault tree analysis. Other nodes may have different CPTs which depend on the relationship of the parents to affect the descendant node. Each node has a CPT, except nodes which do not have parent (initiating event nodes). For these nodes, the occurrence probabilities of their states are assigned which mainly based on statistical data, such as statistical data of the protection component failures of model in figure 5.4.

Table 5.3. CPT of node 'Main protection 2a fail?'

Unit protection 2a or 2b fails?	fail		not fail	
Distance protection 2a fails?	fail	not fail	fail	not fail
Fail	1	0	0	0
Not fail	0	1	1	1

In the event of the local protection P2a fails, P1a can also fail to clear a fault on 0-50% length of line HIGM-RATS if the QB in a state that cause under-reach. The under-reach is also influenced by the type of the faults. Therefore, the model for the protection P1a failure to operate in Z2 time is shown in figure 5.5. In the figure, the protection components are hidden in order to simplify the model and make it easier to follow.

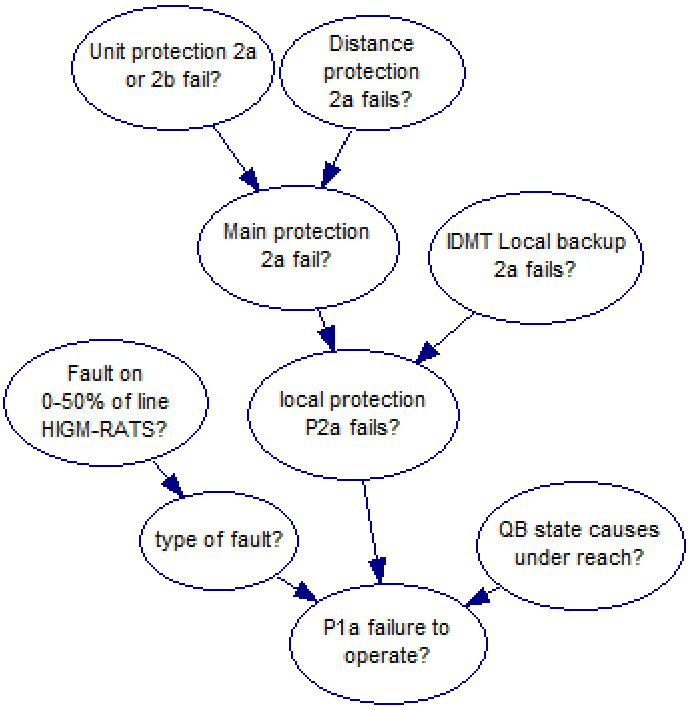

Figure 5.5. Model for failure to operate in zone 2 of the distance protection P1a

Adding consequences of failure to operate in zone 2 time i.e. operate in zone 3 time, the risk model of failure to operate in zone 2 time is shown in figure 5.6. The zone 3 operation time is very long hence it may cause system instability leading to system collapse.

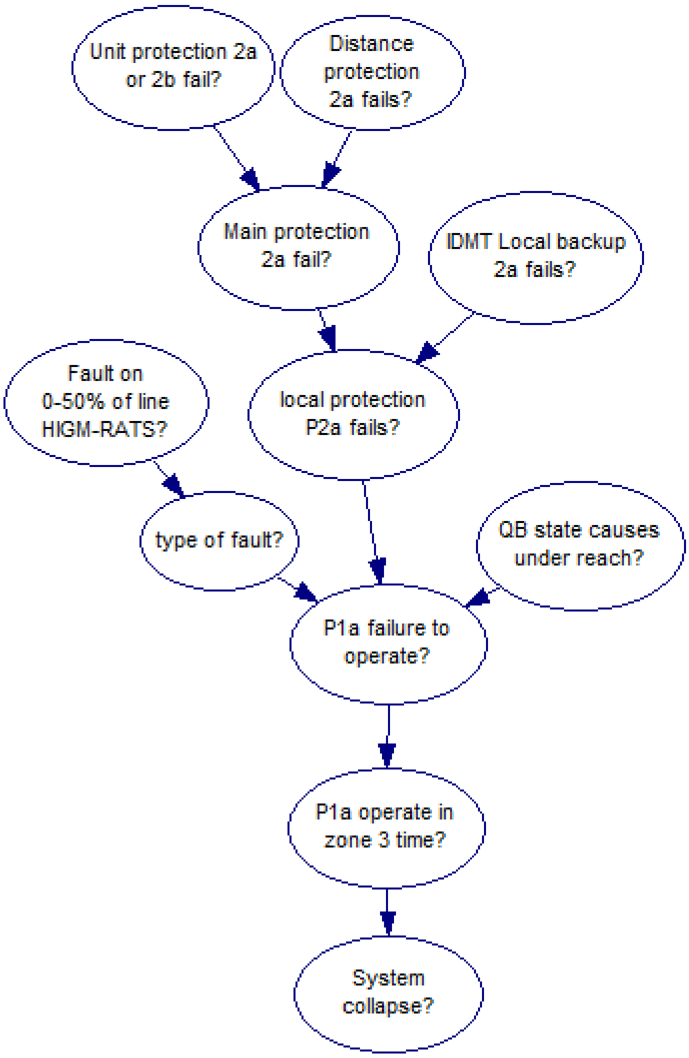

Figure 5.6. Risk model of failure to operate in zone 2 of the distance protection P1a

5.5.2. Model for failure to operate in zone 3 time

As shown in table 5.1, zone 3 operation of the distance protection P1a is for faults located up to 16% length of line RATS-WILE and 6% length of line RATS-STAY. A call for zone 3 operations are initiated by failure of local protection P3a or P3d on line RATS-WILE or P4a on line RATS-STAY then followed by zone 2 operation failure of protection P2a. P1a can fail in zone 3 operation due to under-reach problem during LL faults and QB on buck state. The model of failure to operate in zone 3 is shown in figure 5.7, however the details of protection component failures are not shown to simplify the diagram.

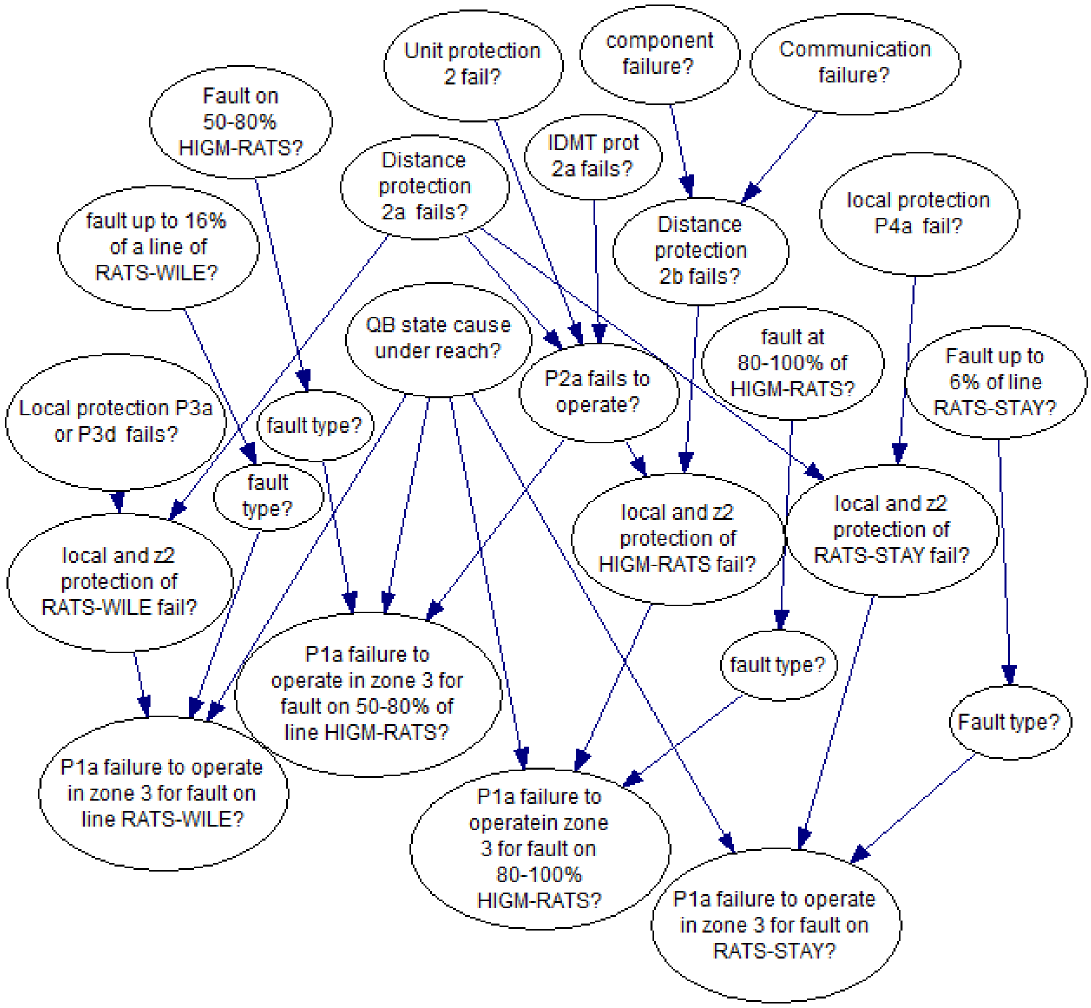

Figure 5.7. Model of failure to operate in zone 3 of distance protection P1a

A failure of protection P1a to provide zone 3 backup can cause a sustained fault in the system, hence it may cause system collapse. Therefore the risk model of distance protection P1a failure to operate in zone 3 is as shown in figure 5.8.

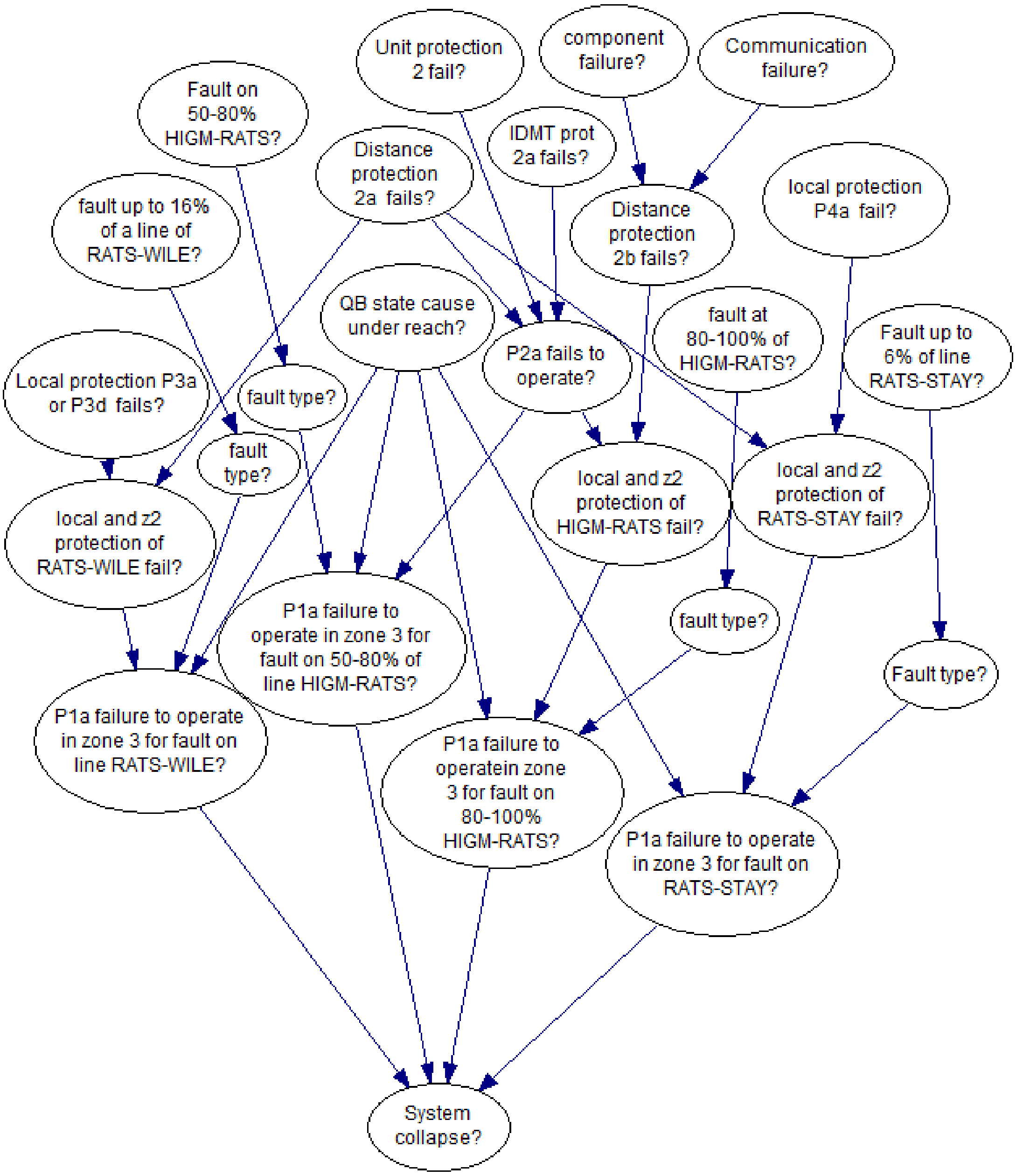

Figure 5.8. Risk model of distance protection P1a failure to operate in zone 3

5.6. Probability of the occurrence of failure modes

The probability metric for the protection failure modes is annual unreliability. This metric is chosen as it expresses annual frequency of failure modes and their consequences. Duration of the failure consequences is based on statistical data and their expected annual duration is calculated as annual unreliability times the statistical duration data which is expressed in equation (4.4). The protection component failure data are gathered from literature, such as the sources presented in chapter 2. As the probability occurrance of the distance protection failure modes is influenced by QB tap states; hence information about probability of each tap of the QB is needed. Since it is assume that the intended operation of the QB is a post fault correction tool, therefore the QB is mainly in the nominal state. Boost taps are intended to drive more power from WBUR generation, while buck taps drive more power from WILE generation as shown by the RTDS simulation result in table 5.4. These simulation results are taken as a basis to calculate the probability of applying of the each QB tap.

Table 5.4. Generator output for different taps of the QB (MW) based on RTDS simulation

Tap of QB	Generator WBUR output	Generator COTT output	Generator WILE output
Boost1	3419	434.4	0
Boost2	3122	498	0
Boost3	2809	568.1	0
Boost4	2483	642.8	0
Boost5	2149	721.9	0
Boost6	1809	804.4	0
Boost7	1468	889.3	76.34
Boost8	1148	971.1	307
Buck1	0	1515	1790
Buck2	0	1450	1624
Buck3	0	1380	1436
Buck4	0	1306	1234
Buck5	192.7	1228	1020
Buck6	489	1146	794.7
Buck7	802.8	1062	400.9
Buck8	1115	979.8	331.4
Nominal state	1125	974.6	730

Boost taps (especially boost1 to boost6) are activated for condition when WILE generation cannot supply the system or is in reduced capacity mode due to generation unit outages. Buck taps are activated for WBUR generation unit outage or partial outage. The probabilities of the generation outages are calculated in term of unavailability of the generator units. WBUR power station consists of 3x435MW Combined Cycle Gas Turbine (CCGT) and 4x500MW coal generation while WILE power station consists of 4x500MW CCGT. The probabilities of total and partial outage of the WBUR power station are calculated using outage data of coal generation unit and CCGT unit in [7] as shows in table 5.5. Similarly for WILE power station is shown in table 5.6.

Table 5.5. Probability of generator unit availability at WBUR power station

Number of unit available	Probability	Corresponding QB state
0	7.1290979e-007	Buck1 to buck4
1	3.3242658e-005	Buck5
2	0.000660	Buck6
3	0.007235	Buck7
4	0.046302	Buck8

Table 5.6. Probability of generator unit availability at WILE power station

Number of unit available	Probability	Corresponding QB state
0	0.00014168	Boost1 to Boost6
1	0.00462768	Boost7
2	0.05668376	Boost8

The taps which share the same generation condition are assumed has uniform probability hence the probabilities are divided equally between the QB taps. Therefore, the QB state probabilities are as shown in table 5.7.

Table 5.7. QB state probabilities

QB state	condition in system	Probability
buck1	WBUR gen total outage	1.78227E-07
buck2	WBUR gen total outage	1.78227E-07
buck3	WBUR gen total outage	1.78227E-07
buck4	WBUR gen total outage	1.78227E-07
buck5	WBUR gen partial outage	3.3242658e-005
buck6	WBUR gen partial outage	0.000660
buck7	WILE gen partial outage	0.007235
buck8	WILE gen partial outage	0.046302
boost1	WILE gen total outage	2.36133E-05
boost2	WILE gen total outage	2.36133E-05
boost3	WILE gen total outage	2.36133E-05
boost4	WILE gen total outage	2.36133E-05
boost5	WILE gen total outage	2.36133E-05
boost6	WILE gen total outage	2.36133E-05
boost7	WILE gen partial outage	0.00462768
boost8	WILE gen partial outage	0.05668376
by pass	Normal	0.884316

In order to calculate probability of the protection under-reach, fault simulation is carried out for each tap of QB, fault position and type of faults using RTDS. From the simulation, the protection's maximum reach for each type of fault and QB tap is obtained. The probability of under reach for faults on a given line, tap of the QB and fault type can be calculated as:

$$P_{under-reach} = \frac{L - maxreach}{L} \tag{5.1}$$

Where

$P_{under-reach}$ = probability of protection under reach for a given QB tap and fault type on a certain line

L = maximum reach of the distance protection when QB on by pass state

$maxreach$ = maximum reach of the distance protection for the QB tap position and the fault type

These under reach probabilities become the input data for nodes of failure to operate which have parent nodes QB state, fault type and failure of local (and backup) protection of the Bayesian network graph in figure 5.6 and 5.8.

5.6.1. Probability of occurrence of failure to operate in zone 2

Probability of zone 2 operation failure occurrence can be calculated using Bayesian network model in figure 5.6. Main protection can only fail if both unit and distance protection fail. If the main protection fails, IDMT back up may operate for earth faults which is around 60% of total fault types or remote distance protection backup may operate for zone 2. The circuit breaker is equipped with circuit breaker fail protection. In the event of the circuit breaker failure, the circuit breaker fail protection will command other circuit breaker(s) to operate and disconnect the fault.

After updating Bayesian Network graph, the results of model in figure 5.6 i.e. the probabilities of protection P1a failure to operate in zone 2 for different QB taps are obtained as shown in table 5.8.

Table 5.8. Probability of protection failure to operate in zone 2 time

QB state	Failure to operate probability
Boost 1	1.49E-10
Boost 2	6.20E-11
Boost 3	2.48E-11
Boost 4	1.24E-11
Boost 5	0.00E+00
Boost 6	0.00E+00
Boost 7	0.00E+00
Boost 8	8.34E-08
Buck1	1.18E-11
Buck 2	1.08E-11
Buck 3	8.22E-12
Buck 4	6.31E-12
Buck 5	8.66E-10
Buck 6	1.04E-08
Buck 7	4.87E-08
Buck 8	9.25E-08

5.6.2. Probability of failure to operate in zone 3

Using RTDS simulation result as input for Bayesian Network model in figure 5.8, the probabilities of zone 3 operation failures are shown in table 5.9. The result shows that the probabilities are very small i.e. -10 order of magnitude or less.

Table 5.9. Probability of failure to operate in zone 3

QB state	Faults on line HIGM-RATS	Faults on line RATS-WILE	Faults on line RATS-STAY
Boost 1	0.00E+00	0.00E+00	8.51E-18
Boost 2	0.00E+00	0.00E+00	8.51E-18
Boost 3	0.00E+00	0.00E+00	8.51E-18
Boost 4	0.00E+00	0.00E+00	8.51E-18
Boost 5	0.00E+00	0.00E+00	1.98E-10
Boost 6	0.00E+00	0.00E+00	1.71E-10
Boost 7	0.00E+00	0.00E+00	9.36E-13
Boost 8	0.00E+00	0.00E+00	0.00E+00
Buck1	5.34E-12	7.08E-14	7.54E-14
Buck 2	3.35E-12	7.08E-14	7.54E-14
Buck 3	1.23E-12	7.08E-14	7.54E-14
Buck 4	3.10E-13	7.08E-14	7.54E-14
Buck 5	1.24E-11	1.32E-11	1.41E-11
Buck 6	0.00E+00	1.78E-10	2.42E-10
Buck 7	0.00E+00	1.13E-09	1.71E-09
Buck 8	0.00E+00	4.61E-10	0.00E+00

5.7. Consequences of protection failure modes

5.7.1. Failure to operate in zone 2

If protection P1a fails to operate as a zone 2 backup for faults on line HIGM-RATS due to the under reach problem, it will operate in zone 3 time. For the most severe under reach condition, the reach of zone 3 is up to 51% of line HIGM-RATS, hence P1a still can cover the zone 2 fault position. Normal zone 3 reach of distance protection on the adjacent line (WBUR-GREEN) is up to 5% of line HIGM-RATS while zone 2 under reach problem of P1a starts from 14.8% of line HIGM-RATS. Therefore, distance protection on the adjacent line cannot provide zone 3 backup for this under reach case.

If zone 3 operating time is assumed still able to maintain system stability, there will be no consequences of P1a zone 2 operation failures. However if zone 3 operating time exceeds system withstand to maintain stability, it will cause cascading effect then leads to blackout. This study uses pessimistic analysis; hence the consequence of failure to operate in zone 2 time is system blackout which its occurrence probability is the same as the failure to operate in zone 2 time (table 5.8)

The cost of system blackout is calculated as total cost of all the generator disconnection plus total cost of all demand disconnection on the system. The cost of generator disconnection consists of two components: profit loss suffered by the generator owner and generator shutdown-start-up cost. For this case study, the duration of the system blackout is assumed for to be two hours, but different durations are calculated for sensitivity study in section 5.9.2. This two hours of disconnection results in hot start of the generation. The cycling cost for hot start is US $59/MW capacity for coal power station and $35/MW capacity for CCGT [8] which is equivalent to £36.10/MW capacity and £21.41/MW capacity respectively in 2011 exchange rates [9]. The profit margin of generation is 20% which is equivalent to £24.08/MWh [10], [11]. Demand disconnection cost is calculated using UK value of loss load (VOLL) which is £16940/MWh [12]. Using these values, the cost of the power system blackout is shown in table 5.10. The difference of the blackout cost for each tap of the QB is due to the difference in prevailing generation mix, amount of each generator output and demand for each tap.

Table 5.10. Consequences of failure to operate in zone 2

QB state	Cost of power system blackout (£)
Boost 1	123,472,109
Boost 2	116,995,519
Boost 3	110,031,645
Boost 4	102,630,315
Boost 5	94,876,459
Boost 6	86,854,825
Boost 7	81,277,627
Boost 8	81,277,264
Buck1	107,775,435
Buck 2	100,673,226
Buck 3	92,726,104
Buck 4	84,049,019
Buck 5	81,215,085
Buck 6	81,223,871
Buck 7	81,233,397
Buck 8	81,277,028

5.7.2. Consequences of failure to operate in zone 3

If protection P1a failure to operate as backup on zone 3, no other backup is available to disconnected the fault. The fault will sustain hence will cause system instability and result in blackout. The probability occurrence of the blackout due to failure to operate in zone 3 is the same with the probability of failure to operate in zone 3 (as in table 5.9). The cost of the blackout is the same as mentioned in table 5.10.

5.8. Risk of the protection failure modes

Risk is calculated as the product of probability and consequences. Using this definition, the risk of the protection failure modes is calculated as product of the probabilities of blackout in table 5.8 and 5.9, and the blackout cost in table 5.10. The calculated risk is shown in table 5.11.

Table 5.11. The Risk of failure to operate of distance protection P1a

QB State	Risk of failure to operate in zone 2 (£)	Risk of failure to operate in zone 3 (£)
Boost 1	1.84E-02	0.00E+00
Boost 2	7.26E-03	0.00E+00
Boost 3	2.73E-03	0.00E+00
Boost 4	1.27E-03	0.00E+00
Boost 5	0.00E+00	0.00E+00
Boost 6	0.00E+00	0.00E+00
Boost 7	0.00E+00	0.00E+00
Boost 8	6.78E+00	0.00E+00
Buck1	1.27E-03	5.91E-04
Buck 2	1.08E-03	3.52E-04
Buck 3	7.62E-04	1.28E-04
Buck 4	5.30E-04	3.84E-05
Buck 5	7.03E-02	3.21E-03
Buck 6	8.46E-01	3.41E-02
Buck 7	3.96E+00	2.31E-01
Buck 8	7.52E+00	3.74E-02
Total	19.21	0.31
Total Risk = £19.51/year		

From table 5.11, it can be seen that the risk of protection failures due to installation of QB on the transmission line is very low: £19.51/year. Although the cost of protection failures is high as it may cause system blackout, the probability occurrence of the protection failures is very low (the highest is in -8 orders of magnitude). The low probability is due to the occurrence of the failure modes only during backup operation. Moreover the main/local protection consists of three independent protections which provide high reliability.

5.9. Sensitivity analysis

Some sensitivity analyses are carried out for different QB tap probabilities and blackout duration. They provide different risk values, as shown in the next sub section.

5.9.1. QB tap probabilities

Since in the base case, it is assumed that the intended operation of the QB is to provide post fault correction, the probabilities of QB states are based on probabilities of power station WBUR and WILE outages. If the intended use of the QB is extended for example alleviation of transmission loading during peak demand, transmission line outages, the probabilities of having QB in boost/buck tap states are increased, the risk of the distance protection P1a failures may also increase. Therefore, sensitivity analysis is carried out for higher probability of the QB taps. The higher probability of each QB tap is obtained by equation (4.1).

$$P(tap)_i = P(tap_{base})_i \times (1 + \alpha) \tag{4.1}$$

Where

$P(tap)_i$ = the new probability of QB tap *i*

$P(tap_{base})_i$ = the base case probability of QB tap *i*

α = a chosen integer to modify the base case probability.

The results for different α are shown in table 5.12.

Table 5.12. Risk for different probabilities of the QB taps

α	Probability of QB on nominal state	Protection failure Risk (£/year)
0	0.884315925	19.51
1	0.768631849	39.00
2	0.652947774	58.55
3	0.537263699	78.03

Table 5.12 shows for condition when around 50% of the time the QB is in boost and buck taps position (α=3), the risk of the distance protection failure is still quite low i.e. £78.03/year. Moreover, these results are obtained for pessimistic assumption that any failures to operate in zone 2 or more always bring the system into blackout. Therefore, it can be concluded that a more frequent engagement of the QB does not bring significant risk to the distance protection.

5.9.2. Blackout duration

Blackout duration is difficult to predict, therefore sensitivity analysis is carried out to calculate the risk for different blackout duration. From the base case 2 hours duration, sensitivity analysis is performed for 1 hour, 3 hour, 5 and 10 hours duration. Different blackout duration results in different generator shutdown-start-up cost due to different type of start (hot, warm or cold start) and different amounts of unsupplied energy, hence the blackout cost will increase with the increasing of the blackout duration. Therefore, the risk of the protection failures will also increase since the risk is a product of the likelihood and the cost of the failures. The sensitivity result is shown in table 5.13.

Table 5.13. Risk of protection P1a for different blackout duration

Blackout duration (hour)	Protection failure risk (£/year)
1	9.78
2 (base case)	19.51
3	29.25
5	48.73
10	97.40

Table 5.13 shows that the increase in blackout duration causes the increase of the quantified risk of the protection failure. However the protection failure risk is still relative low, even for 10 hours of blackout duration. This is due to very low probability of the protection failure modes.

5.10. Conclusion

Utilisation of a QB on a transmission line reduces the reach of distance protection. However, the effect is only for zone 2 and zone 3 operation. Although the consequences of the backup operation failure is high (i.e. can cause system instability), the probability of the protection failure occurrence due to QB operation is very small. Therefore the risk is relatively small, around £19.51/year for the pessimistic assumption. However, if the QB taps areoperated for a significant amount of time, the risk will increase. For operation of 50%, the risk can reach £78.03/year. Similarly, if duration of the blackout due to protection failure mode is increased to 10 hours, the risk can reach £97.40/year. These risk values are quite small considering the importance of 400KV transmission line and the blackout cost. These insignificant risks are caused by very low probabilities of occurrence of the failures. Based on the risk assessment result, existing distance protection can be maintained to protect the transmission line as currently conducted by National Grid. This risk assessment result also demonstrates validation of the methodology.

5.11. References for Chapter 5

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

[2] N. Tleis, *Power systems modelling and fault analysis: theory and practice*: Newnes, 2007.

[3] National-Grid, "Application and Protection Setting Policy for the National Grid UK Transmission System," vol. PS(T)010-issue2, ed. London: National Grid, 2011.

[4] I. F. Abdulhadi, "Facilitating the Validation of Adaptive Power System Protection through Formal Scheme Modelling and Performance Verification," PhD, Electronic aand Electrical Engineering, Strathclyde, Glasgow, 2013.

[5] M. Belivanis and K. R. W. Bell, "Use of phase-shifting transformers on the Transmission Network in Great Britain," in *Universities Power Engineering Conference (UPEC), 2010 45th International*, 2010, pp. 1-5.

[6] RTDS Technologies, "RTDS Manual Set," ed, 2009.

[7] North-America-Electric-Reliability-Corporation, "Generating Availability Report," NERC, Atlanta2012.

[8] N. Kumar, P. Besuner, S. Lefton, D. Agan, and D. Hilleman, "Power Plant Cycling Costs," NREL, Colorado2012.

[9] OANDA. (2011). *Enchange Rates US Dolar to UK Poundsterling 4/8/2011*.

[10] I. MacLeay. (2014, March 2014). Domestic energy bills in 2013: The impact of variable consumption. *Energy trends statistical March*

[11] OFGEM, "The revenue, Costs and Profits of the Large Energy Companies in 2012," London2013.

[12] London-Economics, "The Value of Lost Load (VoLL) for Electricity in Great Britain. Final report for OFGEM and DECC," London Economics, London2013.

Chapter 6. Case study: Finding Optimum Settings for ROCOF Protection

This case study uses the proposed risk assessment framework to find the optimum setting of the distributed generator ROCOF protection for the predicted Great Britain (GB) power system condition in year 2020. The case study is based on the real problem faced by the UK transmission system due to diminishing amount of system inertia. The modelling level of the assessment is quite detail which is based on available data and power system simulation results.

6.1. Background

UK National Grid has proposed to change ROCOF protection current setting in order to anticipate higher Rate of Change of Frequency (ROCOF) experienced in GB power system. The higher system ROCOF is initiated by UK target of 15% energy demand from renewable energy by 2020 [1] . Renewable electricity generation mainly utilises non-synchronous generation technology and therefore does not contribute to power system inertia. As a result, overall power system inertia will decrease and lead to higher system ROCOF.

System inertia is provided by the rotating mass of large synchronous generators. A synchronous generator is designed to operate at specific rotational frequency which is aligned with the nominal system frequency. In the event of system frequency changes due to events, the synchronous generator supplies or increases the stored energy to/from the system using the rotating mass of the turbine shaft to resist any change in speed/frequency. This inherent inertial response helps to diminish potentially fast changes in the overall system frequency and hence acts to reduce the ROCOF. Converter-interfaced generating plants do not have the ability to deliver this inertial response because the absence of the directly connected rotating mass. Asynchronous generators usually have relatively small rotating masses and have no or very little inertia due to different operation design than synchronous generator and the facts that they may be connected through converters which physically decouple the generator from the system.

The higher system ROCOF in the GB system is also triggered by the increase of maximum instantaneous infeed loss from 1320MW to 1800MW which was introduced from April 2014 [2].

Following a large generation loss, system ROCOF can be sufficiently high to cause ROCOF protection to operate to disconnect distributed generation (DG) from the system. If the capacity of affected DGs is high, the cascading effect can lead to system collapse. This unwanted operation of ROCOF protection needs to be prevented by increasing the setting from current setting 0.125Hz/s.

However, higher setting also introduces more chances of undetected Loss Of Mains (LOM) for synchronous machine based DGs, which if sustained, can cause individual safety hazard and out of phase re-closure. Therefore, the trade-off between unwanted operation and failure to operate needs to be considered in choosing the setting. Risk assessment is proposed as a tool to find the optimum setting of ROCOF protection.

Since different failure modes of the ROCOF protection require different scenarios and power systems to be analysed, the next section will describe ROCOF protection and its failure modes. This will be followed by a description of the power systems that are used to analyse the failure modes.

6.2. ROCOF protection and its failure modes

During a LOM condition where a DG is disconnected from the grid, DG is not permitted to continue supplying the rest of the distribution network. Therefore LOM protection needs to be installed to detect and disconnect a DG during LOM condition. One of LOM protection is ROCOF protection.

During normal operation, system frequency will tend to constant or having very small changes therefore ROCOF protection remains stable. However, when a LOM occurs the frequency will increase or decrease because of the unbalance of power in the network hence ROCOF protection will operate if its setting threshold is violated.

The ROCOF experienced by the DG can be calculated as [3]:

$$\frac{df}{dt} = \frac{P_B - P_A}{2\,H\,S} \times f \tag{6.1}$$

Where

df/dt = rated of frequency change in the output of the generator

P_B = generator output before LOM (MW)

P_A = generator output after LOM (MW)

S = nominal rating of the generator (MVA)

H = inertia constant of the generator

f = nominal frequency.

If the system ROCOF exceeds predetermined setting, ROCOF protection will trip, hence disconnecting DG. As ROCOF can also be triggered by other events in the network such as a fault in a nearby line, loss of a generation or load in the system, the stability of ROCOF protection needs to be analysed.

A typical ROCOF relay that is used in the study is based on MiCOM Alstom P341. The relay calculates the average of ROCOF every 3 cycles using the formula:

$$\frac{df}{dt} = \frac{f_n - f_{n-3}}{t_{3\ cycles}} \tag{6.2}$$

In this study, the ROCOF is measured in two type of setting:

- Two consecutive 3 cycle windows with no delay i.e. the relay will trip after two consecutive calculations give result above the setting.
- Two consecutive 3 cycle windows with 500ms delay i.e. adding 500ms delay after the two consecutive calculations. If the calculated ROCOFs in the interval 500ms are remains above the threshold constantly, then the relay will trip.

A ROCOF protection works in time coordination with the autoreclosers in the distribution network hence the ROCOF tripping time must be faster than the dead time of the autorecloser. The ROCOF protection setting according to Distribution Code [4] is the same for all 50MW or less DGs in entire GB power system.

Therefore this study only considers synchronous machine based DG in capacity up to 50 MW and when connected to HV network (11 and 33 kV).

Risk of ROCOF protection comes from its failure to operate during LOM, unwanted operation due to large generation loss and unwanted operation due to nearby faults. The consequences and initiating events of the failure modes are described in section 6.5. while developing the risk models.

6.3. Power systems for case study

Since three failure modes are considered for the case study, each of the failure modes need different analysis and also different power system to be simulated. The failure mode of unwanted operation due to large generation loss requires the GB power system to be simulated. The generation mix and demands are the projected condition for year 2020 which is based on National Grid publication in [5]. A simplified GB power system is used as shown in figure 6.1. The system consists of a responsive synchronous generator, a non-responsive synchronous generator, a tripped synchronous generator, an asynchronous generator, a static load, a dynamic load and a DG. The asynchronous generator is used to represent wind generation with no contribution for system inertia. Details of the system can be found in appendix B

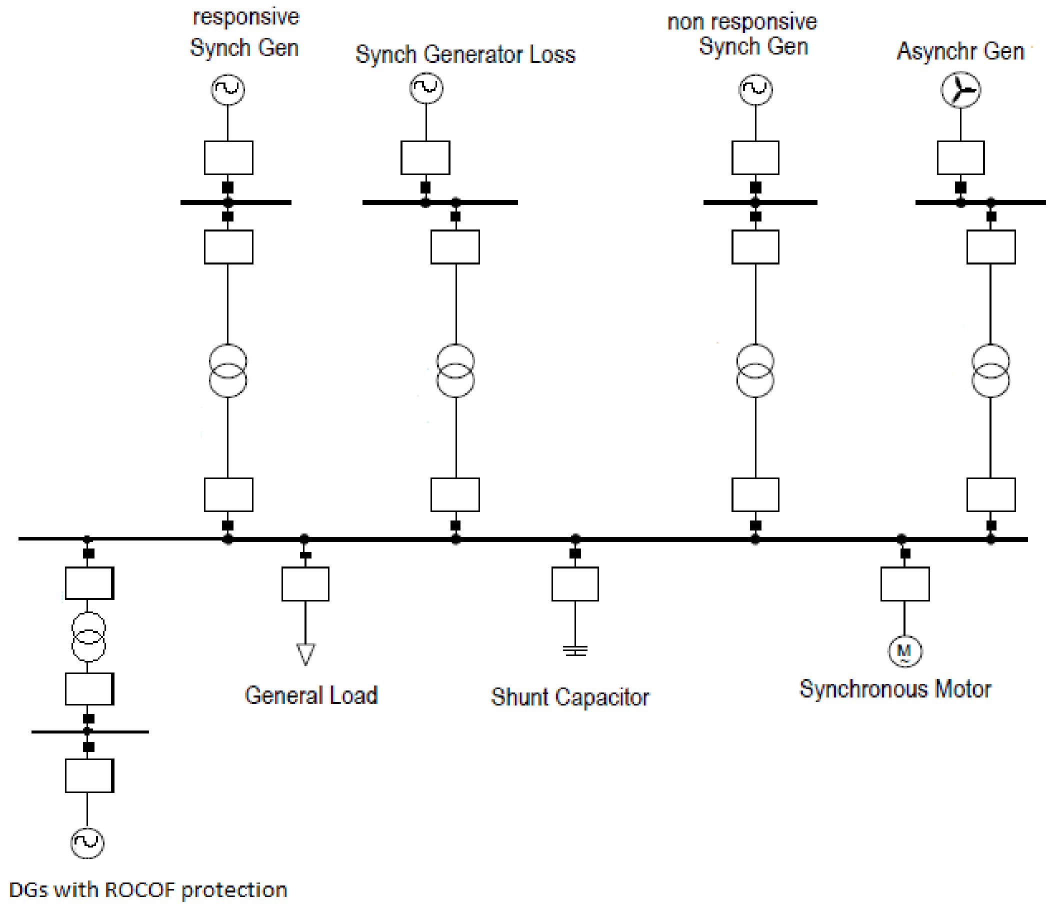

Figure 6.1. The simplified GB power system to simulate the ROCOF protection unwanted operation due to large generation loss

The failure mode of unwanted operation due to nearby faults requires simulation of faults in a distribution network with DG to examine whether the occurrences of faults on the network cause unwanted operation of the ROCOF protection. The UKGDS1-EHV1 (United Kingdom Generic Distribution Network System1-Extra High Voltage1) is used [6]. The system is developed by the Centre for Distributed Generation and Sustainable Electrical Energy, collaboration between the University of Strathclyde and the University of Manchester. The system represents a 33 kV rural distribution network which is fed from 132 kV supply point. A DG is placed at bus 318 as shown in figure 6.2. to represent a DG with ROCOF protection. The detail of the distribution network components can be found in appendix C.

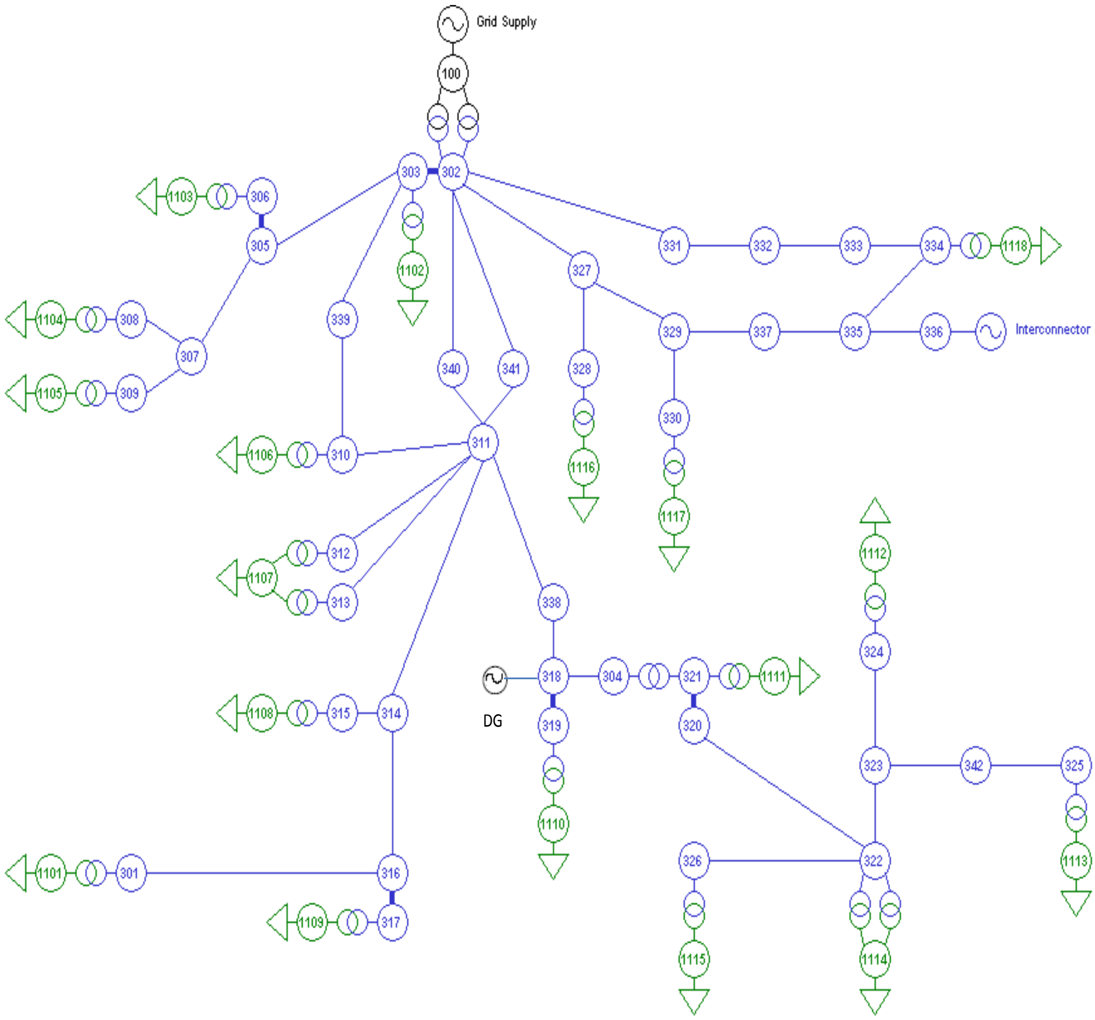

Figure 6.2. The simulated system for unwanted operation due to nearby faults [6]

For failure mode of "failure to operate", the simulation results are taken from the study conducted by Dysko et al. in [7]. The study employed two distribution networks i.e. 33 kV and 11 kV as shown in figure 6.3. and 6.4. respectively. The study used three load profiles recorded from urban and rural substations to examine the possibility of the DG output being balanced with the local demand at particular points in time and over different durations. Detail of the networks can be found in [7]

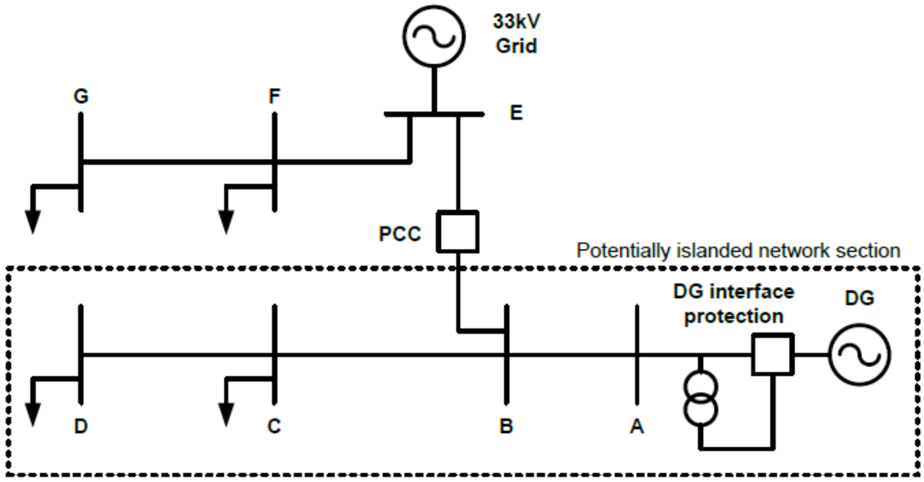

Figure 6.3. 33 kV test network for the failure to operate [7]

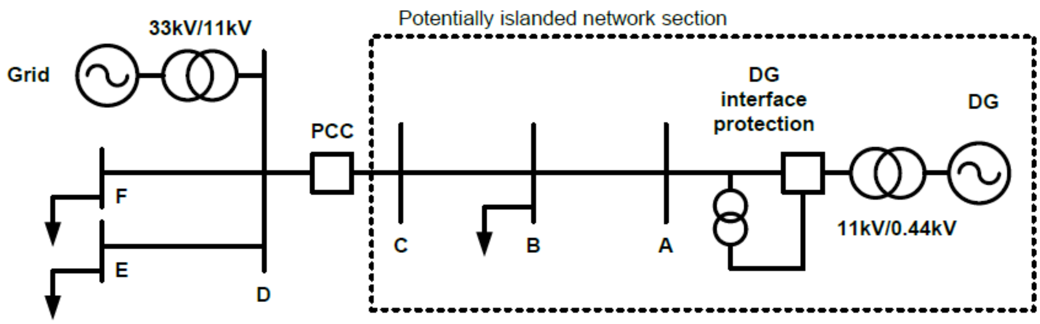

Figure 6.4. 11 KV test network for the failure to operate [7]

6.4. Assumption, limitations, metrics and data used in the assessment

As the aim of the study is to find the optimum setting, the considered initiating events are only those affected by the setting. The risk due to protection component failures is not influenced by the setting. This risk remains the same for any chosen setting. Therefore the protection component failures are excluded from the assessment. The study also assumes that the dead time of autorecloser is 20 seconds hence the duration of islanding operation can only sustain for 20 seconds (or maximum 40 seconds in case first reclose is successful). The typical dead times of autorecloser that are employed by distribution network operator, are between 3 seconds to 20 seconds [8]. The maximum dead time i.e. 20 seconds is taken to quantify the risk of the worst condition (the longest duration of the islanding) which has safety hazard consequence as explained later in section 6.5.

Since the component failures of the ROCOF protection are ignored in the assessment, the assessment results can only be used for conditions where the component failures do not contribute significantly for decision making. If for example the intended use of the assessment is for comparing the risk of different protection schemes, the protection component failures will contribute significantly; therefore these case study results cannot be used.

The assessment will calculate the annual probability of the ROCOF protection failure modes and consequences in form of unreliability metric. The duration of the consequences are based on statistical data from National Grid publication. The risks will be calculated in form of annual risk cost in UK pound sterling/year.

Most of the statistical data have been gathered from National Grid publication/ website. If the required data cannot be found from National Grid publication, similar data from other publications are used. DIgSILENT Power Factory [9] is employed to simulate power system scenario and the simulation results are also used as a source of the assessment data.

6.5. Developing models for ROCOF protection risk

In this section, risk models for each of these failure modes is developed while considering the objective of finding optimum setting for ROCOF protection. The risk model proceeds continuously from the initiating events to the final consequences of the failure mode.

6.5.1. Modelling the risk of failure to operate during LOM

Failure to operate during LOM can cause sustained islanding. The sustained islanding can cause danger of [10,11]:

- Damage of the network and customer's electrical equipment caused by uncontrolled frequency and voltage.
- Damage of generator, turbine and transformer due to out of synchronism automatic reclosing operation.
- Safety hazard for maintenance personnel as no earthing arrangements are in place in the island and also because the personnel believe that the network is not energized.
- Faults in the islanding network may remain undetected because of the protection is not designed for islanding condition.

From these consequences of sustained islanding, Bayesian network model for failure to operate as shown in figure 6.5

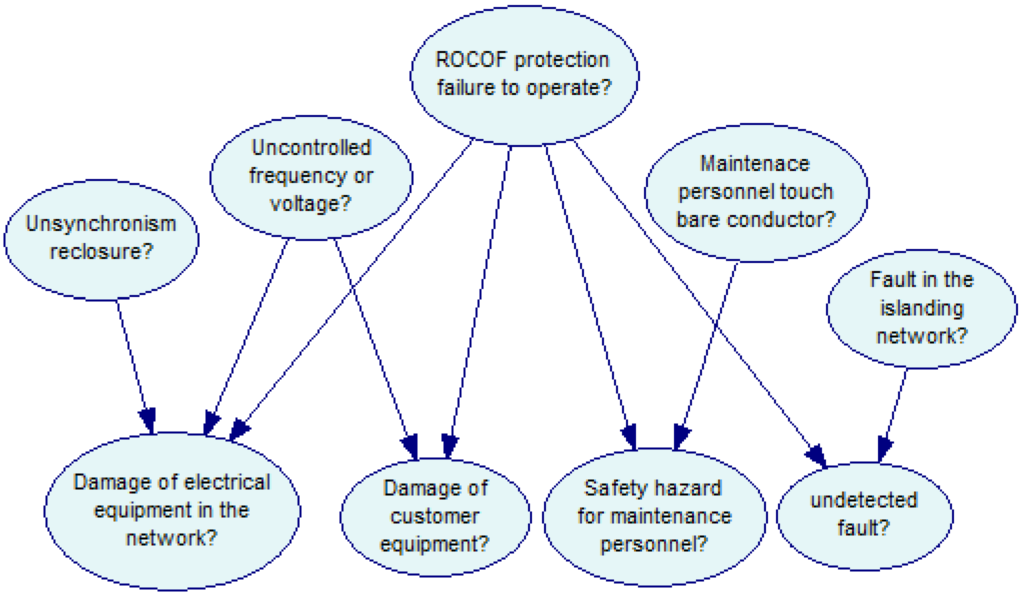

Figure 6.5. Impact of a ROCOF protection failure to operate

Initiating events of the protection failure to operate are:

- LOM event
- Protection component failures
- Undetected LOM (Non-detected Zone/NDZ) because of very small or no frequency changes due to the balance of local demand and DG output during LOM.

Adding these two initiating events, the Bayesian network is as shown in figure 6.6.

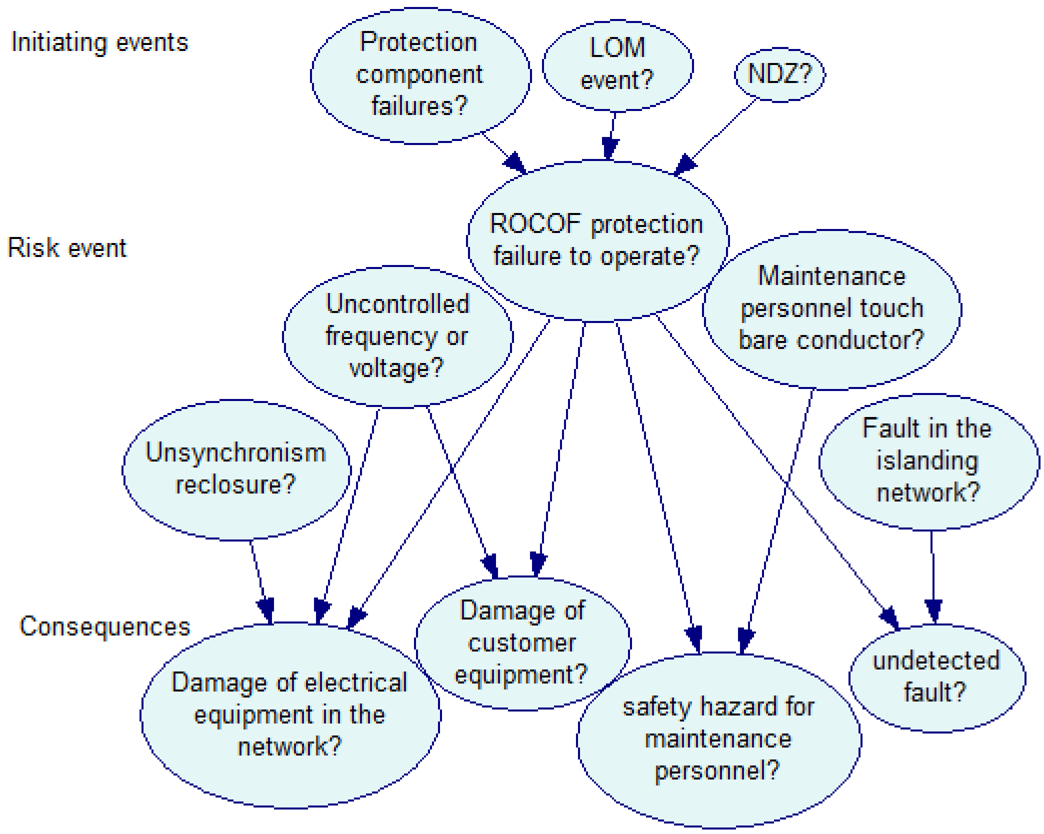

Figure 6.6. Risk model of a ROCOF protection failure to operate

The protection component failures initiating event can be eliminated from the model as stated by assumption in section 6.4. Since the remaining initiating events are LOM event and NDZ, the only condition which causes the protection failure to operate is the constancy of the frequency (otherwise NDZ will not happen). This brings an implication that a fault in the islanding network cannot remain undetected because the fault will cause change in the frequency then trigger the operation of ROCOF protection thus terminate the islanding. As a result, node 'undetected fault?' and node 'Fault in the islanding network?' must be eliminated from the model. Furthermore, as DGs are equipped with over and under voltage relays along with over and under frequency relays [10], in the event of frequency or voltage magnitude exceeding the limits, the relays will trip the DG, hence islanding condition will ceased. Therefore node 'Uncontrolled frequency or voltage' and its descendant can be eliminated from the model. The revised model is as shown in figure 6.7.

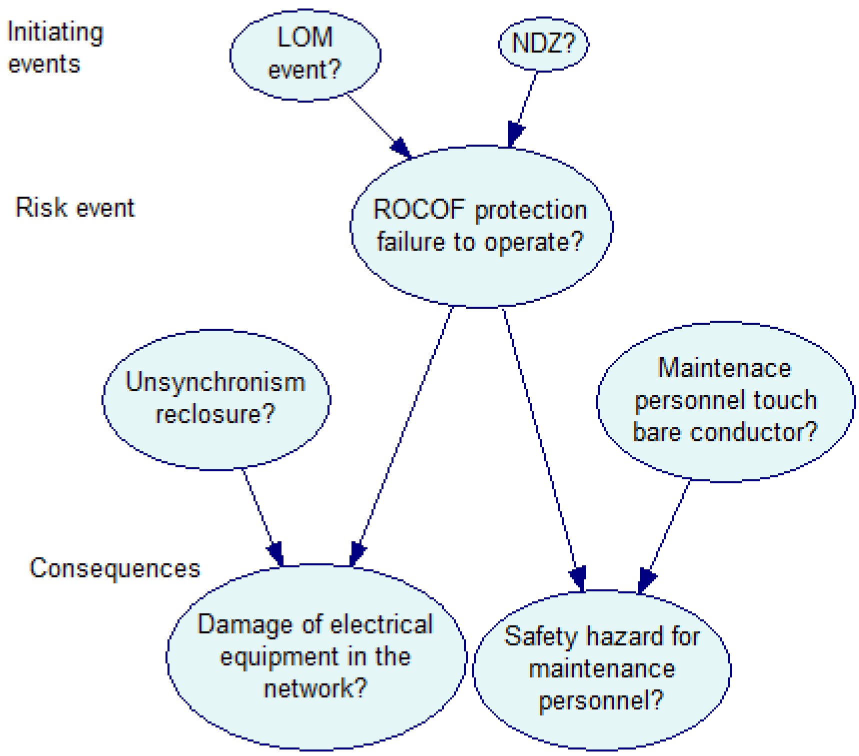

Figure 6.7. Risk model 1 of protection failure to operate for finding optimum setting study

The NDZ happens if the local demand is equal (or closed to) in terms of active and reactive power to the DG output. Three seconds duration of the power balance is taken based on the minimum time to reclose of an autorecloser [8]. Therefore the node 'NDZ' can be substituted with node 'DG output balances with local demand for 3s or more?'.

A DG does not operate all the time. As the probability of DG output in balance with and local demand is assumed base on constant output of DG with 100% load factor, then a node 'DG operates' is added. This node represents the probability of finding a DG in operating condition. Therefore, the risk model in figure 6.7 is modified as shown in figure 6.8.

The safety hazard in terms of fatalities or injury is mainly caused by unearthed islanding network. The low voltage networks have earthing system but no earthing system in HV network during islanding condition. Consequently, the safety risk occurs in a HV network and the network is only accessible by electrical worker. Therefore, the accident only happens if there is a worker in vicinity of HV network during islanding condition, and the worker touches a faulty metal surface. As the probability of maintenance personnel touches bare conductor depends on their presence in vicinity of the HV network then node 'Maintenance personnel is in vicinity of a HV network' is added as a parent node as shows in figure 6.8.

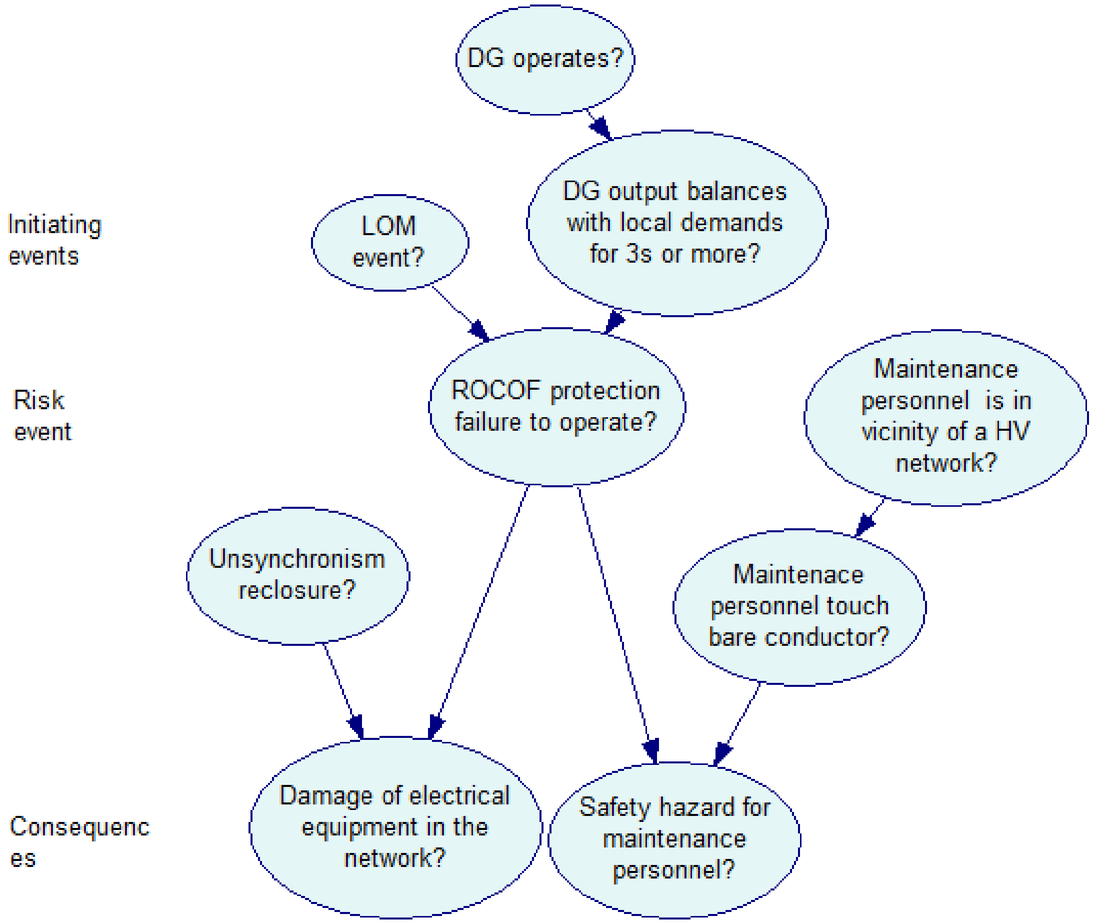

Figure 6.8. Risk model 2 of protection failure to operate for finding optimum setting study

Since islanding conditions can only occur if there is enough reactive power supply from the DG along with active power supply for the local load, then the islanding DG needs capability to produce reactive power. Therefore, for this study, it is assumed that islanding operation only happens for synchronous generation technology of DG. There are some types of DGs which utilise synchronous generator such as hydro power, biomass and CHP.

6.5.2. Modelling the risk of unwanted operation

A ROCOF protection can trip for any events which causes frequency changes. The initiating events of frequency changes are large generation loss, large demand loss and a fault in other networks nearby.

The initiating event of a large generation loss can result in high system ROCOF in the whole system hence numerous DGs may be tripped by their ROCOF protection if ROCOF exceed the setting. Depend on the amount of tripped DG capacity; the system frequency may continue to fall and result in operation of demand under frequency protection. Amount of demand disconnection due to the operation of demand under frequency protection is proportional to the fall of system frequency. In the worst case if the disconnected demand is insufficient to arrest the frequency fall then it may lead to system collapse. This cascading effect is illustrated in a model of ROCOF protection unwanted operation risk in figure 6.9a.

The initiating event of a fault on a nearby network to the DG can cause a high ROCOF event and result in ROCOF protection trip and disconnect the DG. This event is local and amount of generation loss is relatively small and can easily be replaced by other generation. However the probability of its occurrence is high as fault occurrences in distribution network are high. Therefore this failure mode is included in the analysis. The probability of unwanted operation is also influenced by DG condition i.e. in operation or not. The unwanted operation risk model is shown in Figure 6.9b.

The initiating event of a large demand loss may also cause a high ROCOF event hence can trip the DGs. However the DG loss has positive effect for balancing the system after the demand loss. Therefore, it is assumed the consequences are relatively small and this initiating event will not be considered in this study.

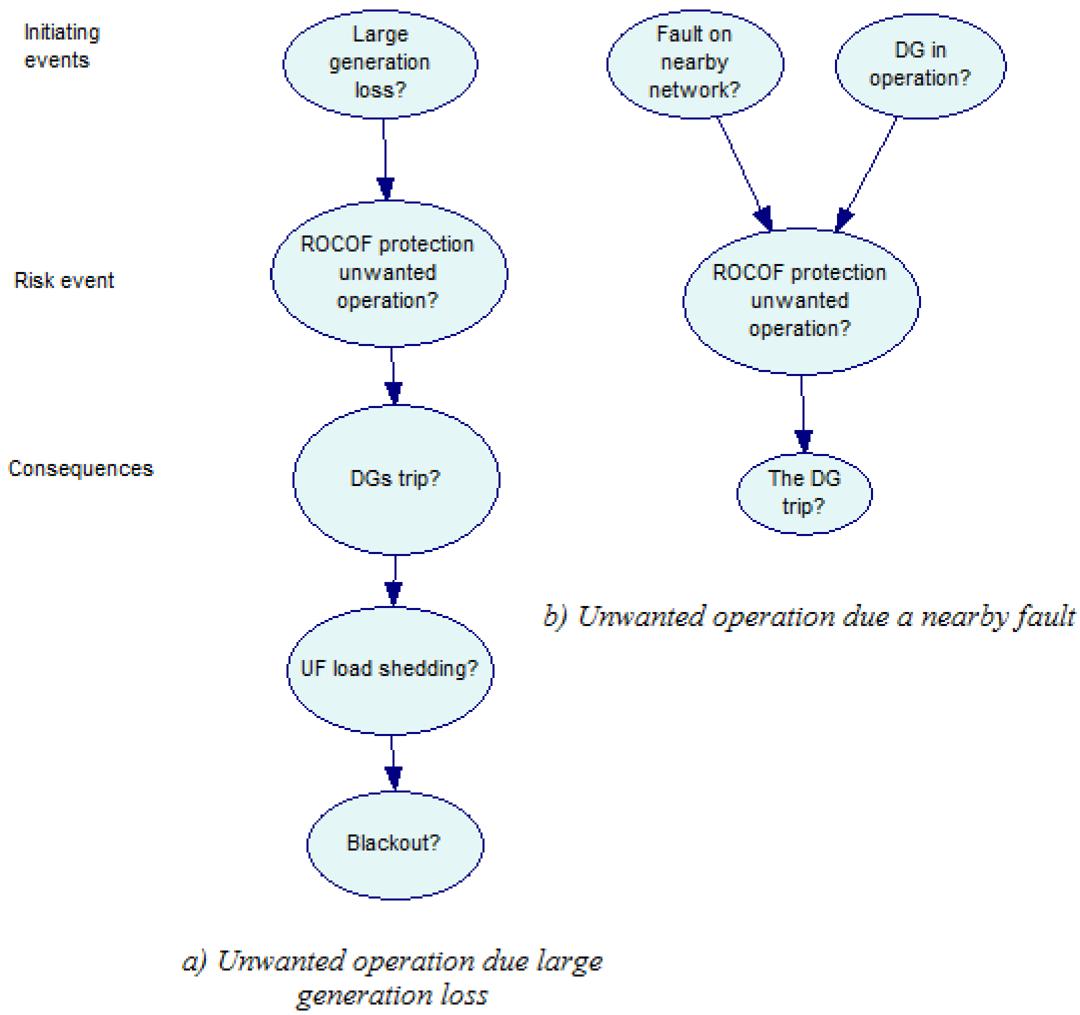

Figure 6.9. Risk model of ROCOF protection unwanted operation

The occurrence of unwanted ROCOF protection operation due to large generation loss is influenced by the amount of the generation loss, demand level and wind level during the loss. The wind level represents the level of non-synchronous generation technology in the GB power system, since the main non-synchronous generation technologies come from wind generation [13]. Other non-synchronous renewable generation, such as solar energy, is still relatively insignificant compared to the wind generation, although this may change in the future [13].

For the same amount of generation loss, low demand produces higher ROCOF because the system has less generation hence provides less inertia. Similarly, higher wind level condition also becomes a factor of higher ROCOF because more wind generation could be supplying the system. As most of wind generation are non-synchronous machine technologies, they do not contribute to system inertia; hence the system will have less inertia and is more prone to higher ROCOF events. Adding these two factors, the risk model in figure 6.9a is revised into the risk model in the figure 6.10. An additional connection is included between node ‘Low demand?’ and node ‘UF load shedding?’ as the amount of demand disconnection depends on total demand at the time of incident.

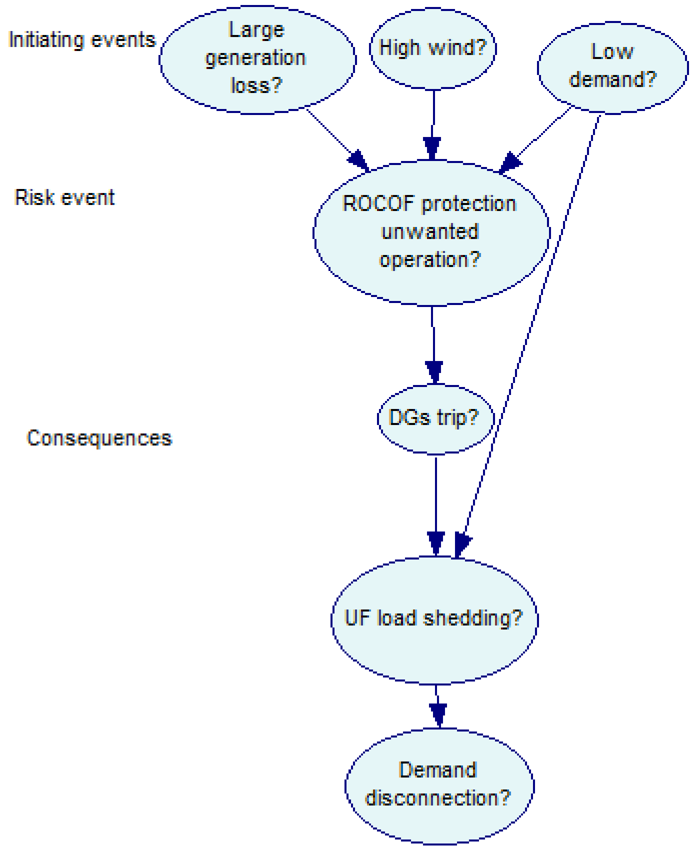

Figure 6.10. Risk model of protection unwanted operation due to large generation loss

6.6. Probability of ROCOF protection failure modes

6.6.1. Probability of unwanted operation due to generation loss

In order to calculate the probability of unwanted operation due to large generation loss, probabilities of the initiating events have to be calculated. The following section will explain about the probabilities of these initiating events.

6.6.1.1. The initiating event of large generation loss

Large generation loss is defined on the basis of maximum infeed loss criteria of National Grid [8] which considered generation losses from 1300MW to 1800MW. The range of 1300-1800MW is divided into 5 equal interval with the size of 100MW. Sources of these generation losses are based on data of:

- Transmission Entry Capacity (TEC) of single unit larger than or equal to 1300MW [13]
- a group of generation connected thru single line having capacity equal or larger than 1300MW [12].

The node “large generation loss” in Figure 6.10 can be expanded as in figure 6.11 to include the causes i.e. nuclear and wind generation loss. There are 3 new nuclear power stations with TEC 1600MW or more which will in operation in 2020. Each of these plants can introduce risk of loss generation up to 1800MW if the reactor experiences instantaneous full-load trips. Additionally, seven single HVDC transmissions with each capacity larger than or equal to 1800MW which is connected in radial to offshore wind farms will pose large generation loss risk if the transmission line experiences any faults. The list of the large generation loss sources is shown in table 6.1.

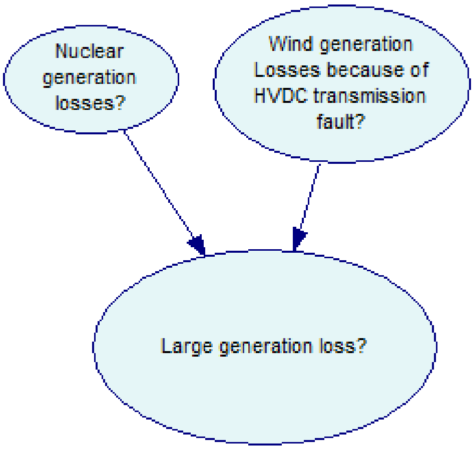

Figure 6.11. Parent nodes of "Large generation loss" node

Table 6.1. Sources of 1300-1800MW generation loss

No	Source	Amount of loss (MW)	Generation capacity (MW)
1	Hinkley point C Nuclear plant	1700 - 1800	1670
2	Oldburry on Severn Nuclear plant	1700 - 1800	1600
3	Sizewell C (stage 1) Nuclear plant	1700 - 1800	1670
HVDC transmission from:			
4	Firth of Forth offshore wind farm toTealing	1300 - 1800	3690
5	Hornsea offshore wind farm to Killingholme	1300 – 1800	2500
6	Moray Firth offshore wind farm to Peterhead	1300 – 1800	2650
7	Doggerbank offshore wind farm to Creyke Beck	1300 - 1800	5500
8	Greenwire onshore wind farm to Pembroke	1300 – 1500	1500
9	Marex offshore wind farm to Connahs quay	1300 – 1500	1500
10	Irish Bridge Tranche 2 to Alverdiscott	1300 - 1400	1400

Nuclear power plants usually have their output greater than registered TEC to provide electrical power for their own facilities in the plants. Therefore, a nuclear plant loss can cause a generation loss amount equal to the TEC plus additional power for the plant facilities which is supplied by the grid. As a result the three nuclear plants can cause a loss of between 1700MW to 1800MW [12]. The probability of the nuclear generation loss is determined by the nuclear reactor fault. Other faults may cause a large generation loss but the probability is in smaller order of magnitude as other nuclear plant's components always have one or more backup [14]. Faults on the substation of the nuclear plant rarely cause generation loss due to layout of the substation which allows the continuity of supply in the event of occurrence a fault. Each nuclear power reactor experiences unplanned full load trip once every nine years [12], hence the loss failure rate is 1/9 fault per year and the loss probability is :

$$P = 1 - e^{-\lambda t} \tag{6.3}$$

$$P_{nuclear} = 1 - e^{-1/9} = 0.105161 \text{ pa}$$

The offshore wind farms, although possessing generation capacities higher than 1800 MW, are restricted to a maximum output that they can deliver to the system of 1800 MW. This condition is regulated by infrequent infeed loss criteria from National Grid [12]. For each of the seven HVDC transmissions, the influence factors of the large generation loss occurrence are: the probability of a wind farm output is more or equal to 1300MW, probability the wind farm in operation, and probability of the HVDC transmission cable experiencing a fault. The Bayesian Network of the large generation loss caused by HVDC transmission loss is shown in figure 6.12. Only cable fault is considered in the HVDC transmission since other component faults (converters at each end for example) will most likely not cause full capacity loss [12].

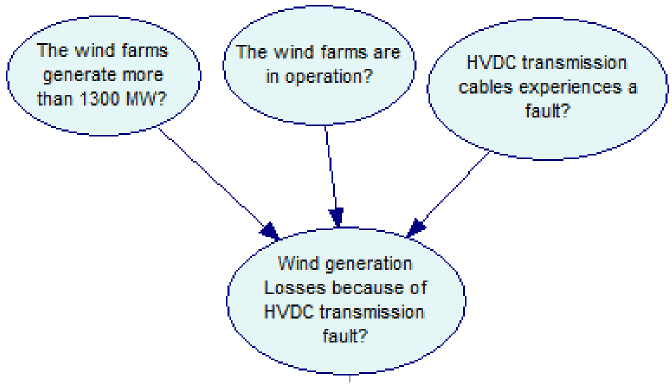

Figure 6.12. Bayesian network for large generation loss caused by HVDC transmission

The probability of the node “wind farm in operation” in figure 6.12 is based on loading factor of wind generation: 0.3 pa [15]. The node “HVDC transmission cable experiences a fault” has the probability occurrence once in 10 years [12] or the failure rate 1/10 pa, hence the cable fault probability :

$$P_{HVDC} = 1 - e^{-1/10} = 0.095163 \text{ pa}$$

The node “the wind farm generates power more or equal to 1300MW?” has the probability based on percentage of long term average output of wind distribution [16]. The probability is based on the blue line graph shown in figure 6.13. For each output interval of the wind farm, the capacity factors are calculated. The capacity factor result is fitted to the line graph in figure 6.13 to obtain the probability of its occurrence. The results are output intervals and their probabilities of occurrence as shown in table 6.2. For the wind farms with the capacity a lot of higher than 1800MW, the probability to generate an output interval 1700-1800 MW will be very significant compared to wind farms with lower capacity.

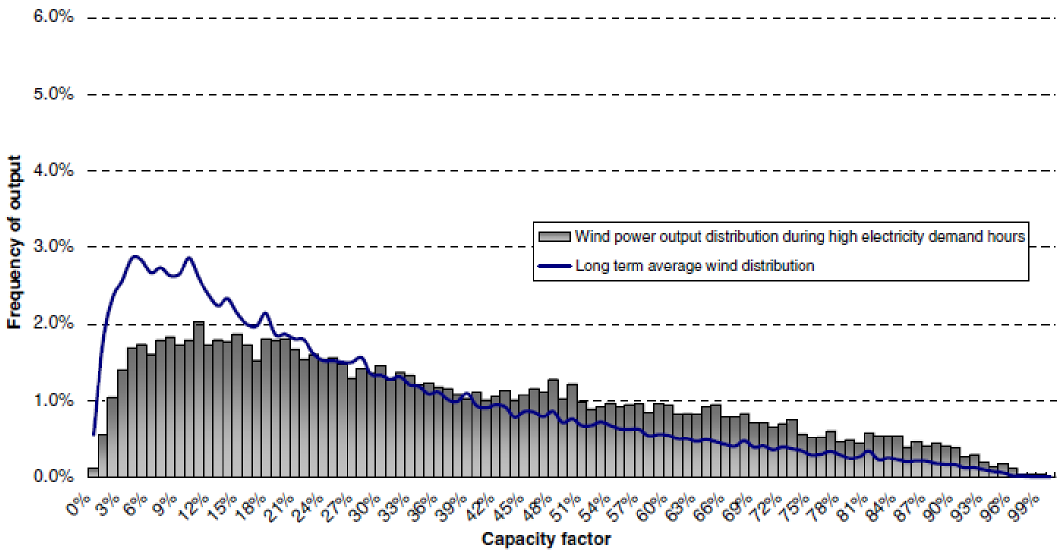

Figure 6.13. Long term average output of wind distribution [12]

Table 6.2. Probabilities of wind farm output level

Wind farm and capacity	Output interval (MW)	Capacity factor of the output interval	Probability occurrence of the wind farm output interval
Firth of Forth offshore wind farm, 3690MW	1700 - 1800	> =0.461	0.2315625
	1600 - 1700	0.434 - 0.46	0.02625
	1500 - 1600	0.407 - 0.4336	0.028125
	1400 - 1500	0.38 -0.4065	0.020625
	1300 - 1400	0.35 - 0.379	0.031875
Hornsea offshore wind farm, 2500MW	1700 - 1800	>=0.68	0.075625
	1600 - 1700	0.64 - 0.68	0.018125
	1500 - 1600	0.6 - 0.64	0.02125
	1400 - 1500	0.56 - 0.6	0.02375
	1300 - 1400	0.52 - 0.56	0.0328125
Moray Firth offshore wind farm, 2650MW	1700 - 1800	>=0.642	0.093125
	1600 - 1700	0.604 - 0.6415	0.02125
	1500 - 1600	0.566 - 0.604	0.0178125
	1400 - 1500	0.528 - 0.566	0.02625
	1300 - 1400	0.49 - 0.528	0.0278125
Doggerbank offshore wind farm, 5500MW	1700 - 1800	>= 0.309	0.4225
	1600 - 1700	0.29 - 0.309	0.0265625
	1500 - 1600	0.273 - 0.29	0.0284375
	1400 - 1500	0.255 - 0.273	0.03
	1300 - 1400	0.24 -0.26	0.045
Greenwire onshore wind farm, 1500MW	1400 - 1500	>=0.93	0.00328125
	1300 - 1400	0.87 - 0.93	0.0186875
Marex offshore wind farm, 1500MW	1400 - 1500	>=0.93	0.00328125
	1300 - 1400	0.87 - 0.93	0.0186875
Irish Bridge Tranche 2 wind farm, 1400MW	1300 - 1400	>=0.93	0.004375

For each wind farm, the probabilities of the intervals in Table 6.2 are assigned into the node 'The wind farm generates more than 1300MW?' at Figure 6.12. An example of calculation the Bayesian Network for the Firth of Forth offshore wind farm is shown in figure 6.14. The probability of wind farm in operation is based on the generic loading factor of wind farms i.e. 0.3 [17]. The probability of the HVDC transmission cable experiences a fault is 0.095163 per year as calculated in the previous section.

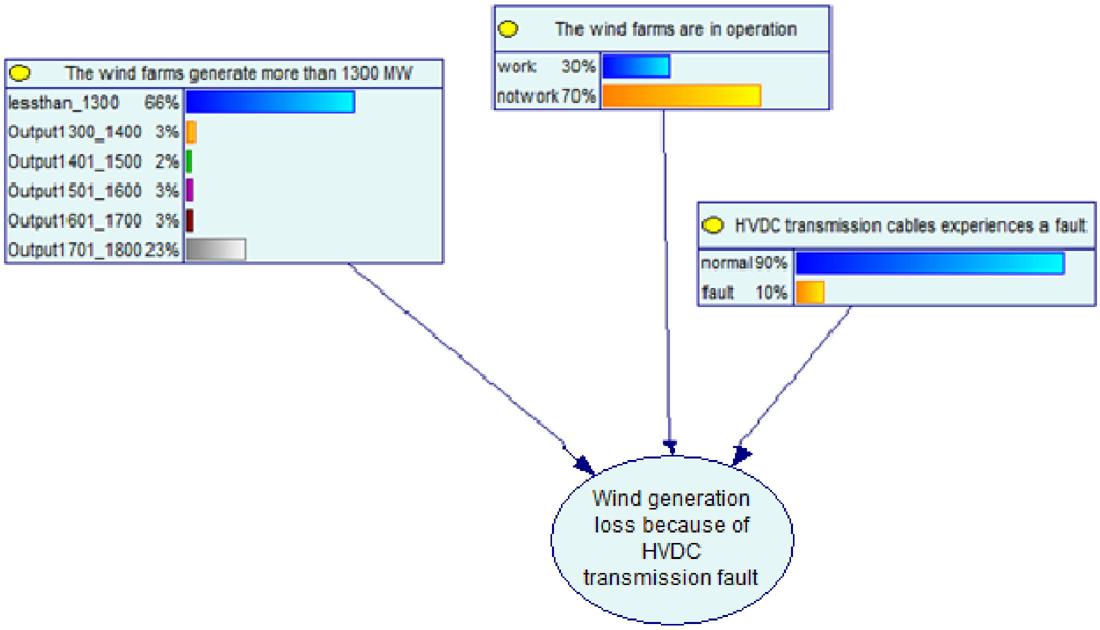

Figure 6.14. Bayesian Network of Firth of Forth offshore wind farm generation loss

After running the Bayesian Network software, the generation loss probability for Firth of Forth wind farm is as shown in the third row of table 6.3. Similar Bayesian Network for other wind farms give the probability of generation loss interval as shown in table 6.3. In table 6.3 the probabilities of nuclear generation loss are also included. Total probability loss for each interval is shown at the bottom of the table.

These intervals and their total probabilities are assigned into the node 'Large generation loss?' in the risk model in figure 6.10.

Table 6.3. Probabilities of generation loss interval

Power Plant	Loss Interval (MW)					
	1700-1800	1600-1700	1500-1600	1400-1500	1300-1400	Less than 1300
Firth of Forth	0.006611	0.000749	0.000803	0.000589	0.000910	0.990338
Hornsea	0.002159	0.000517	0.000607	0.000678	0.000937	0.995102
Moray Firth	0.002659	0.000607	0.000509	0.000749	0.000794	0.994683
Doggerbank	0.012062	0.000758	0.000812	0.000856	0.001285	0.984227
Greenwire	0	0	0	0.000094	0.000534	0.999373
Marex	0	0	0	0.000094	0.000534	0.999373
Irish Bridge Tranche 2	0	0	0	0	0.000125	0.999875
Hinkley point C	0.105161	0	0	0	0	0.894839
Oldbury on Severn	0.105161	0	0	0	0	0.894839
Sizewell C (stage1)	0.105161	0	0	0	0	0.894839
TOTAL	0.338974	0.002631	0.002731	0.00306	0.005119	0.647485

6.6.1.2. The initiating event of low demand

National Grid's Gone Green Scenario predicted that GB peak demand and total annual demand in year 2020 will be slightly low than current demand due to increasing energy efficiency [17] as shown in figure 6.15 and 6.16.

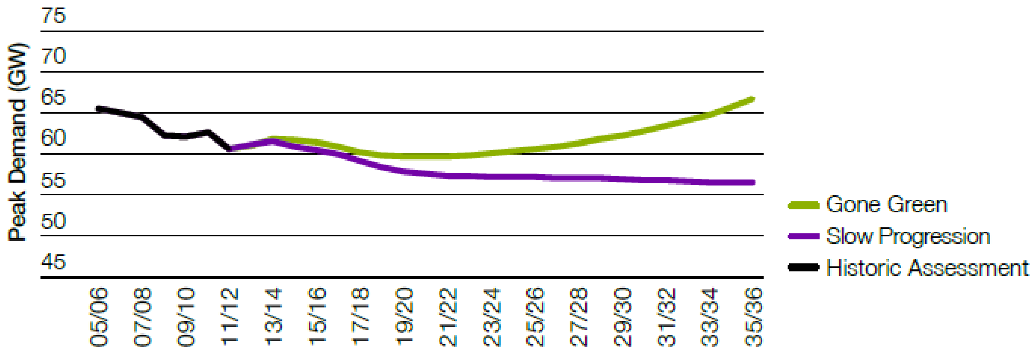

Figure 6.15. Forecast of GB peak electricity demand [13]

Figure 6.16. Forecast of GB total annual electricity demand [13]

As this study needs information about the probability of occurrence of the demand levels, the available historical data i.e. for year 2008 to 2010 [5] are used. The data are shown in figure 6.17. It is assumed that these data can represent percentage demand level for year 2020.

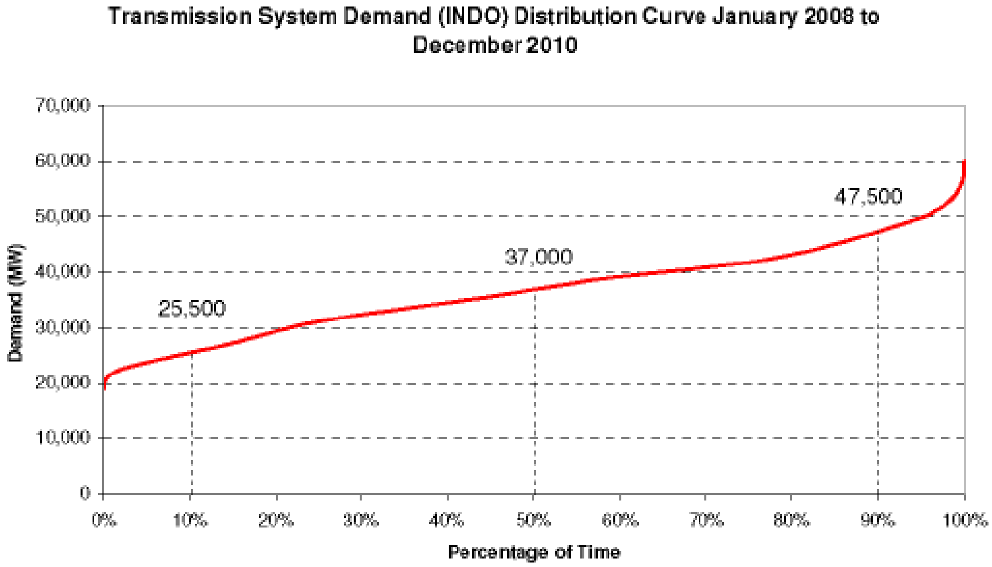

Figure 6.17. Transmission system demand cumulative distribution curve [14]

From figure 6.17, the minimum demand is 20GW and the maximum demand is nearly 60GW. In this study, demand considered is from 20GW to 55GW and divided into eight intervals as shown in table 6.4. The probability occurrence of the demand interval as shown in table 6.4 is based on data from figure 6.17. These probabilities of the demand intervals are assigned into the node 'Low demands?' in the risk model in figure 6.10.

Table 6.4. Probability of the occurrence of electricity demand

Median	demand (GW)	Probability
20	17.5 -22.5	0.027
25	22.5 - 27.5	0.123
30	27.5 - 32.5	0.16
35	32.5 - 37.5	0.226
40	37.5 -42.5	0.237
45	42.5 -47.5	0.117
50	47.5 - 52.5	0.078
55	>=52.5	0.032

6.6.1.3. The initiating event of high wind

Wind generation level is based on data in generation mix scenario for year 2020 in National Grid report [5]. In the report, the high wind level is defined for wind generation output from 60% to 90% of the wind farm capacities, while the average level is from 30% to 40% and low level is from 0% to 5%. For the purpose of this study, the wind level is assumed as 'high' if it is equal or higher than 60% of the wind generation capacity, 'average' if it is 30% to 60 % of the capacity and 'low' if it is less than 30%. The occurrence probabilities of the wind level are based on data in the graph of long term average wind output in Figure 6.13. The probabilities of the wind levels are shown in table 6.5 and they are assigned into the node 'High wind' in figure 6.10.

Table 6.5. Wind level probabilities

Wind level	Probability occurrence
High	0.1125
Average	0.346875
Low	0.540625

6.6.1.4. System ROCOF due to large generation loss

In order to gather the information about ROCOF experienced in the system after large generation loss, DIgSILENT Power Factory software has been utilised to simulate GB system in figure 6.1. Generation mixes for various demands are based on Gone Green Scenario for 2020 from National Grid [5]. The asynchronous generator is used to represent wind generation with no contribution for system inertia.

The simulation is carried out for every combination of demand level, wind level and amount of generation loss. An example of the frequency trace from the simulation result for 1800MW generation loss during 20 GW system demand and high wind condition is shown in figure 6.18 and the corresponding system ROCOF is in Figure 6.19. These results have been verified to the report of National Grid in [5].

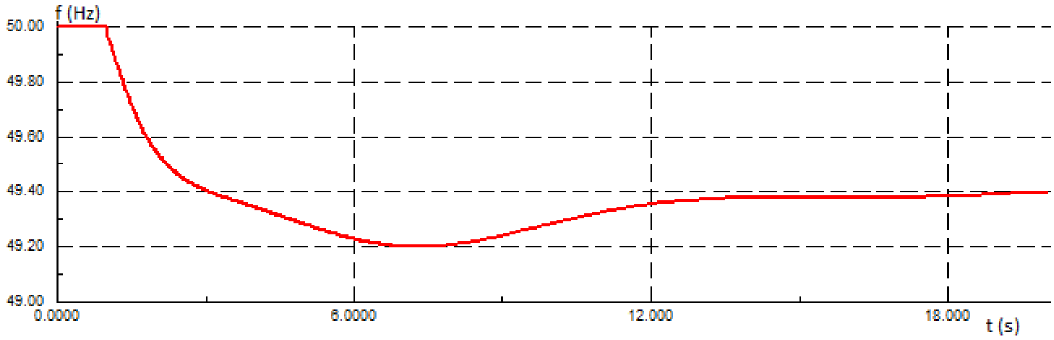

Figure 6.18. Simulated frequency fall for 1800MW generation loss, 20GW demand and high wind

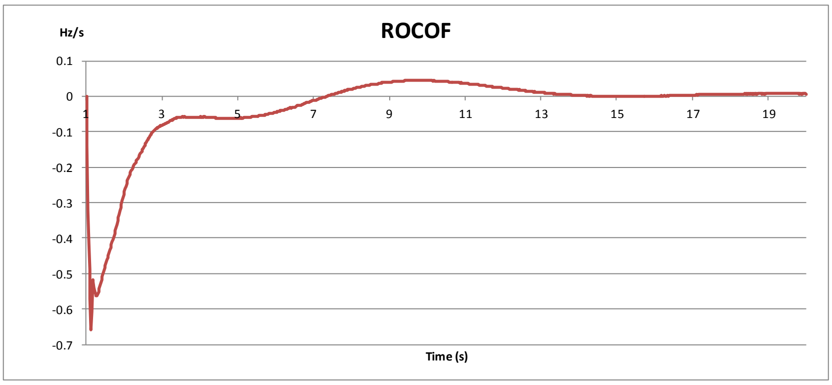

Figure 6.19. Simulated ROCOF for 1800MW generation loss, 20GW demand and high wind using 6 cycle average window

The ROCOF results from the simulation are compared with the chosen ROCOF protection setting to decide whether the protection will trip or not. If the ROCOF value under specified operating time-delay is higher than the setting, then the protection will trip with probability one. However, if the value is equal with the setting then the probability of trip is 0.5 and for value which is less than the setting, the probability of trip is zero.

The simulation is carry out for 1800, 1700, 1600, 1400 and 1320 MW generation loss and the ROCOF protection will trip if the measured ROCOF is higher than the setting. Examples of the simulation results for 20GW demand are shown in table 6.6.

Table 6.6. ROCOF protection with 0.3Hz/s no delay setting

Demand	Wind condition	Generation loss (MW)					
		1800	1700	1600	1500	1400	1320
20 GW	High	Trip	Trip	Trip	Trip	Trip	Trip
	Average	Trip	Trip	Trip	-	-	-
	Low	-	-	-	-	-	-

As the generation loss is presented in form of 100MW intervals as shown in table 6.3, for the interval which has the upper value cause the protection trip but the lower value does not, then the probability of the protection trip will be less than one but greater than zero. The trip probability for the interval calculates as illustrated in figure 6.20. A and B are the lower and upper bounds of the generation loss interval respectively. For A MW generation loss, the ROCOF experienced is lower than the protection setting, but for B MW generation loss, the ROCOF is higher than the setting. The ROCOF is exactly the same with the protection setting for C generation loss. C is obtained from interpolation using TREND function in Microsoft Excel software. Then the probability of the relay trip for the AB interval can be calculated as:

$$p = \frac{B - C}{B - A} \tag{6.4}$$

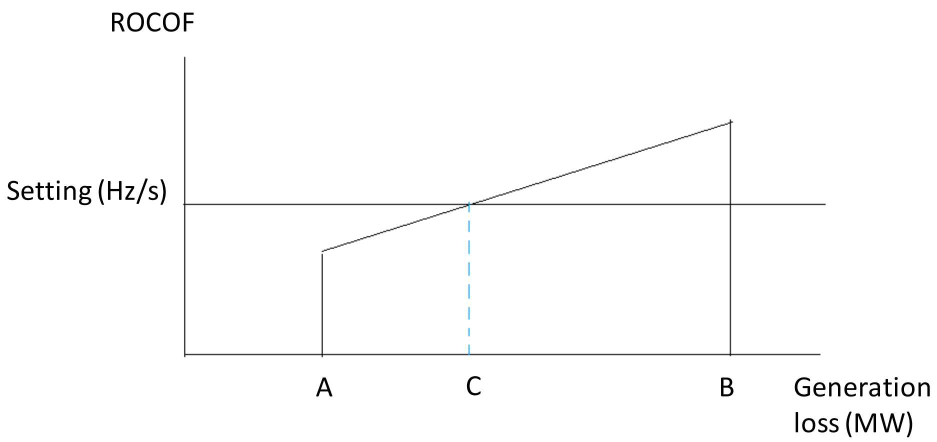

Figure 6.20. The ilustration for the calculation of ROCOF protection trip probability for a generation loss interval

Then based on the recorded results, the probability of the protection trip is assigned into the node 'Protection unwanted operation?' of the risk model in figure 6.10. An example of the probabilities value for 20GW demand and 0.3Hz/s no delay setting is shown in table 6.7.

Table 6.7. Probability of ROCOF relay trip for various wind condition and generation loss and the relay setting: 0.3Hz/s no delay

Demand	Wind condition	Generation Loss (MW)					
		1700-1800	1600-1700	1500-1600	1400-1500	1300-1400	less or no loss
20 GW	High	1	1	1	1	1	0.157804554
	Average	1	1	0.10427628	0	0	0
	Low	0	0	0	0	0	0

After all the nodes data has been assigned, the results of Bayesian network model in figure 6.10, are as shown in table 6.8. The no delay setting of 0.6Hz/s or higher do not experience any unwanted operation and similarly for 500ms delay setting of 0.5Hz/s or higher. From these results, it can be concluded that high settings, higher than the possible ROCOF due to maximum generation loss, can prevent unwanted operation of the ROCOF protection. Applying a delay may also increase the stability of the ROCOF protection. However the high setting and delay may cause undetected LOM if the unbalance between local load and DG output is relatively small. This will be verified in section 6.6.3.

Table 6.8. Probabilities of unwanted operation of ROCOF protection caused by large generation loss

Setting (Hz/s)	Setting no delay	Setting 500ms delay
0.3	0.025521369	0.01202438
0.4	0.011194925	0.00103305
0.5	0.001034332	0
0.6	0	0
0.7	0	0
0.8	0	0
0.9	0	0
1	0	0

6.6.2. Probability of unwanted operation due to nearby fault

The probability of unwanted operation due to nearby fault is calculated based on fault simulation of UKGDS-EHV1 for rural network [6] as shown in figure 6.2. and more detail in appendix C. A 30MW synchronous machine based DG is added to the network. Numerous fault simulations using DIgSILENT Power Factory are carried out in different places of the network in order to measure ROCOF in the network following a fault. It is found that for the same fault location three phase faults cause higher ROCOF value than phase to phase fault. Phase to phase faults result in higher ROCOF value than single phase to ground faults.

Model for risk of unwanted operation due to nearby fault is shown in figure 6.9b. The frequency of occurrence of faults on the UKGDS system is calculated for every line, transformer and bus in the system and based on fault data from [18]. It is found that the frequency of fault occurrence is 11.965 fault/year for the UKGDS, which consist of 2.195 three phase faults, 4.283 phase to phase faults and 5.487 one phase to ground fault. Since DG average loading factor is 0.5895 (see Appendix C) hence the frequency of failure that can cause ROCOF protection operation to disconnect the DGs are the failure occurrence frequencies times the loading factor. The results are shown in second column i.e. 'affected fault/year' of table 6.9.

As the fault frequencies are larger than one fault/year, the probability of fault occurrence (unreliability) for a year mission time is not a suitable metric for this case. Although the model in figure 6.9b is used, the calculation is not carried out using Bayesian Network, instead simple multiplication using parameter failure rate is implemented.

DIgSILENT fault simulations are carried out at each line end, transformer and node. From the simulation, ROCOF values seen by the protection are compared with the chosen settings in order to decide whether the protection will trip or not. For each type of fault, the percentage of the unwanted trip is calculated. An example of results for setting 0.4Hz/s no delay is shown in table 6.9. Multiplication of these percentages (second column) to affected fault/year (first column) result in fourth column i.e. number of unwanted trip/year. Number of the unwanted trip/year for all fault type is shown at the bottom row. Similarly, numbers of unwanted trip for different settings are shown in table 6.10.

Table 6.9. Number of unwanted operation for setting 0.4Hz/s no delay

Fault type	affected fault/year	trips during the faults	trip/year
Three phase fault	1.294062347	85%	1.10002459
Phase to phase fault	2.525012528	85%	2.14640034
One phase to ground	3.234575585	76%	2.45843744
Total trip/year due to fault near by			5.70486237

Table 6.10. Number of unwanted operation due to nearby faults

Setting	Number of unwanted trip/year	
	no delay	500ms delay
0.3Hz/s	5.704862	5.575108
0.4Hz/s	5.704862	5.20198
0.5Hz/s	5.575108	4.674861
0.6Hz/s	5.322607	4.336381
0.7Hz/s	5.160878	4.03877
0.8Hz/s	4.818635	3.922316
0.9Hz/s	4.68986	3.556705
1Hz/s	4.560477	3.195056

From results in table 6.10, it can be seen that applying higher settings give less number of unwanted operations. Adding a 500ms delay results in further reduction of the unwanted operation. However in general, delay and higher setting cannot completely prevent the unwanted operation due to nearby faults in the distribution network. Moreover, the higher setting may cause undetected LOM condition.

6.6.3. Probability of failure to operate

Results of the study by Dysko et all in [7] are used in this thesis in order to calculate the failure to operate risk of ROCOF protection in different settings. Modification has been made to the probability metric by applying unreliability metric as in equation (6.3).

Based on Risk model in Figure 6.4, the risk of ROCOF protection failure to operate is calculated. For the convenience Figure 6.8 is shown again in figure 6.21 for part of calculating failure to operate probability. Node ‘DG operates?’ in the figure has two states: operate and not operate. The probability of operate state is based on average loading factor of synchronous machine technology DGs as calculated in appendix B and is shown in table 6.11.

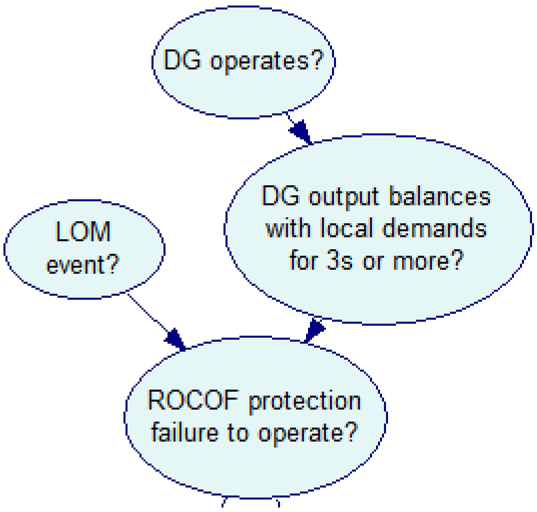

Figure 6.21. Bayesian Network model for calculating the probability of ROCOF protection failure to operate

The probabilities of the DG output balances with local demand for three second or more are based on study in [7] which uses three load profiles recorded from urban and rural substations. The three load profiles give different probabilities and the average of them is used. DG output balance with local demand for 3s or more has the probability as shown at CPT in table 6.12 for setting 0.5 Hz/s no delay.

Table 6.11. Probability table of node ‘DG operates?’ in figure 6.21

States	Probability
Operate	0.589538368
Not operate	0.410461632

Table 6.12. CPT of node 'DG output balances with local demands for 3s or more?'

DG operates?	Operate	Not operate
Balance	0.0379	0
Not balance	0.9621	1

Table 6.12 shows that when node 'DG operate?' is in the operate state, the probability the DG output in balance with the local demand is 0.0379. When DG is in 'not operate' state, the probability of DG output in balance with local demand is zero.

The frequency of losing of supply in primary substation based on data in [7] is 0.0375 per year. Consequently, the probability of losing of supply in primary substation is:

$$P_{LOM} = 1 - e^{-0.0375} = 0.036805582$$

This value is used for the probability of node 'LOM event?' in figure 6.21. Then the CPT of node 'ROCOF protection failure to operate?' is as shown in table 6.13. From the table, ROCOF protection will fail with probability 1 if DG output in balance with local demand for 3s or more and the LOM event occurs

Table 6.13. CPT of node 'ROCOF protection failure to operate'

DG output balances with local demands for 3s or more	Balance		Not balance	
LOM event	Occur	Not occur	Occur	Not occur
Fail	1	0	0	0
Not fail	0	1	1	1

After updating the data at the Bayesian Network (figure 6.21), the probability of the ROCOF protection failure for a setting of 0.5 Hz/s with no delay is 0.000822. Similarly, the probabilities of the protection failure to operate for different settings are shown in table 6.14.

From the results in table 6.14, it can be concluded that higher setting cause higher probability of ROCOF protection failure to operate. Applying delay also causes a higher chance of undetected LOM. This condition is opposed with the unwanted operation failure modes, therefore a compromise can be found using the quantification of the failure mode consequences in risk assessment.

Table 6.14. Probability of ROCOF protection failure to operate

Setting (Hz/s)	No delay	500ms delay
0.3	0.000381054	0.000745650
0.4	0.000606202	0.000992914
0.5	0.000822366	0.001241143
0.6	0.001118025	0.001487443
0.7	0.001386184	0.001734707
0.8	0.001653893	0.001981971
0.9	0.001911894	0.002229235
1	0.002160187	0.002476500

6.7. Consequences of the protection failure modes

6.7.1. Consequences of the protection unwanted operation due to large generation loss

It is estimated that around 4GW DG capacity can be tripped by the higher system ROCOF event. This capacity based on DG capacity prediction for 2020 [19] and applying current condition where around 50% of synchronous machine based DG have ROCOF protection [8].

Based on recorded data of system frequency during large generation loss in 2012 [8, 20], it is concluded that the high ROCOF can be experienced in the whole GB system, not only in the nearby area of the large generation loss. The power system frequencies are recorded at three universities i.e.: University of Strathclyde in Glasgow, University of Manchester and Imperial College in London [21]. Three generation loss incidents, shown in table 6.15, are used to analyse the effect of generation loss on power frequency in different area. The traces frequencies of the incidents are shown in figure 6. 22, 6.24 and 6.26, also the average ROCOF measured over 500 ms is shown in figure 6.23, 6.25 and 6.27. It can be seen from figure 6.23 that a loss in England causes high ROCOF that can also be experienced in Glasgow in similar magnitude. Similar condition is shown in figure 6.22 and 6.23 for incident number 2 and 3 respectively.

Table 6.15. Incidents of generation loss in 2012 [8, 20]

No	Date	Time	Size loss	Loss	Location
1	28 Sept 2012	01:48	1000MW	France Interconnector tripped	South England
2	14 Marc 2012	15:10	1000MW	France Interconnector tripped	South England
3	2 March 2012	20:14	1260MW	Sizewell B tripped	South East England

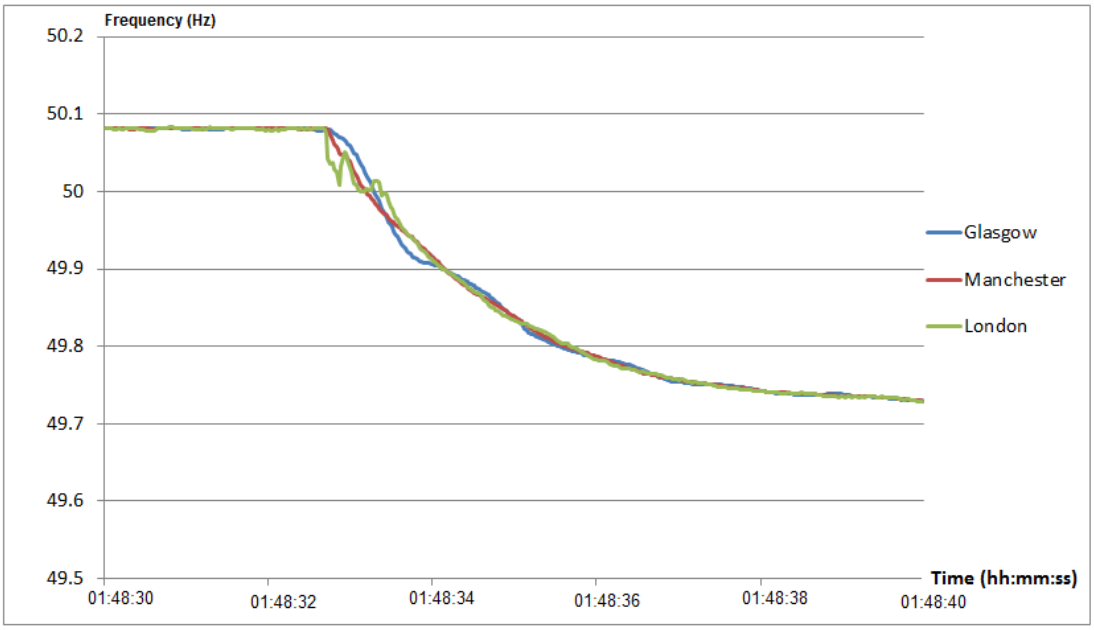

Figure 6.22. Frequency traces during 1000MW Interconnector loss on 28 Sept 2012 [21]

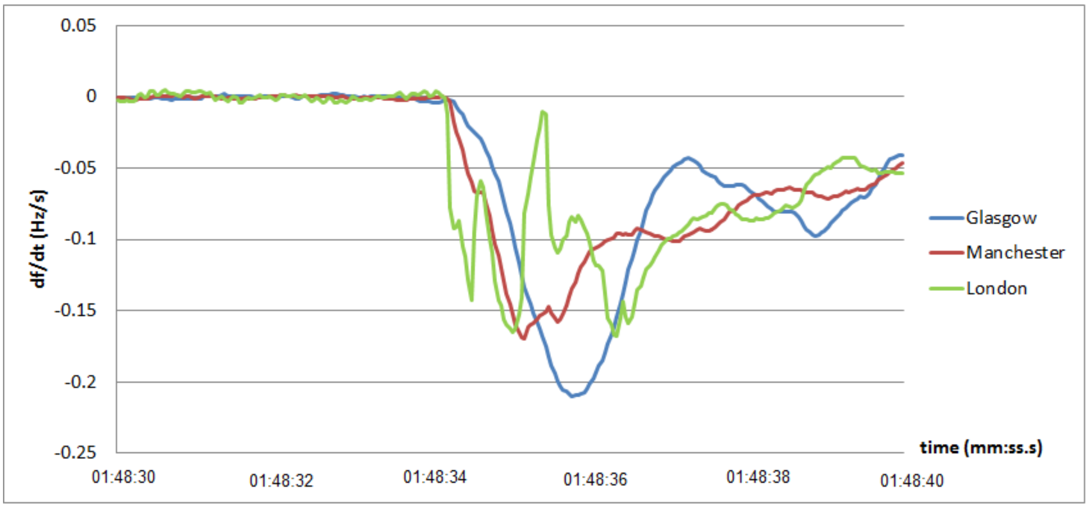

Figure 6.13. Average over 500 ms ROCOF of 1000MW Interconnector loss on 28 Sept 2012

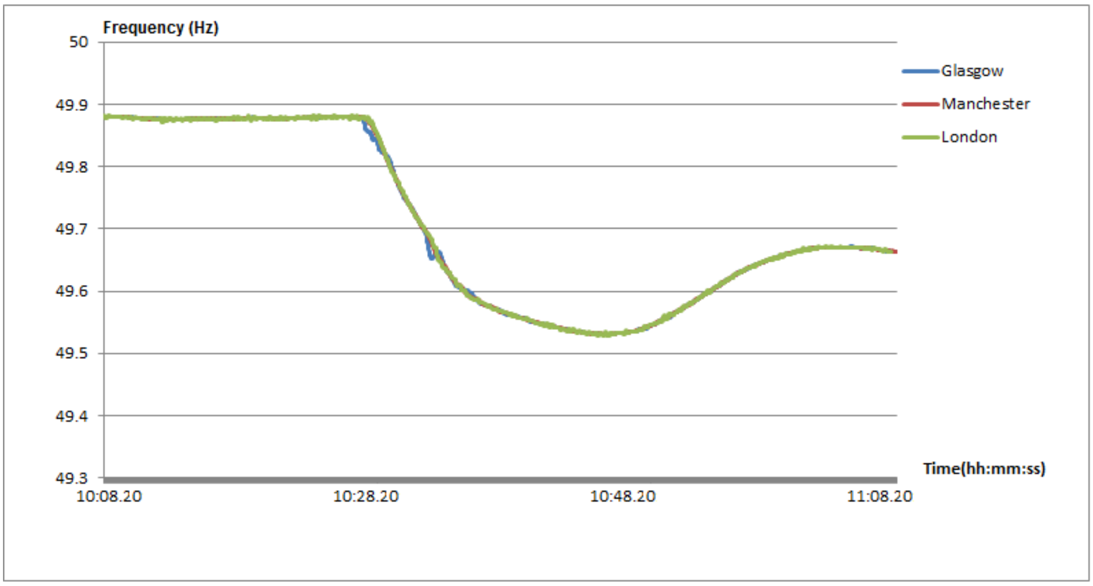

Figure 6.24. Frequency traces during 1000MW Interconnector loss on 14 March 2012 [21]

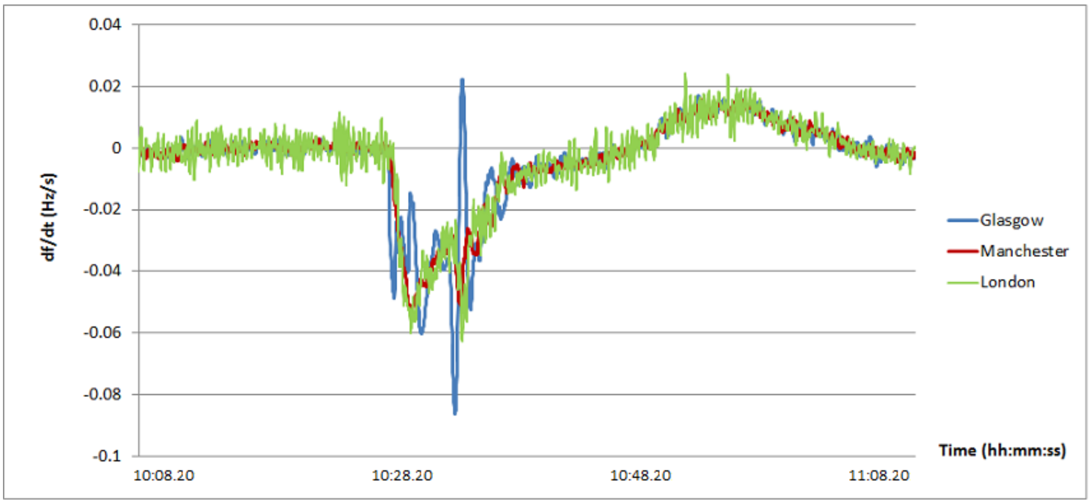

Figure 6.25. Average over 500 ms ROCOF of 1000MW Interconnector loss on 14 March 2012

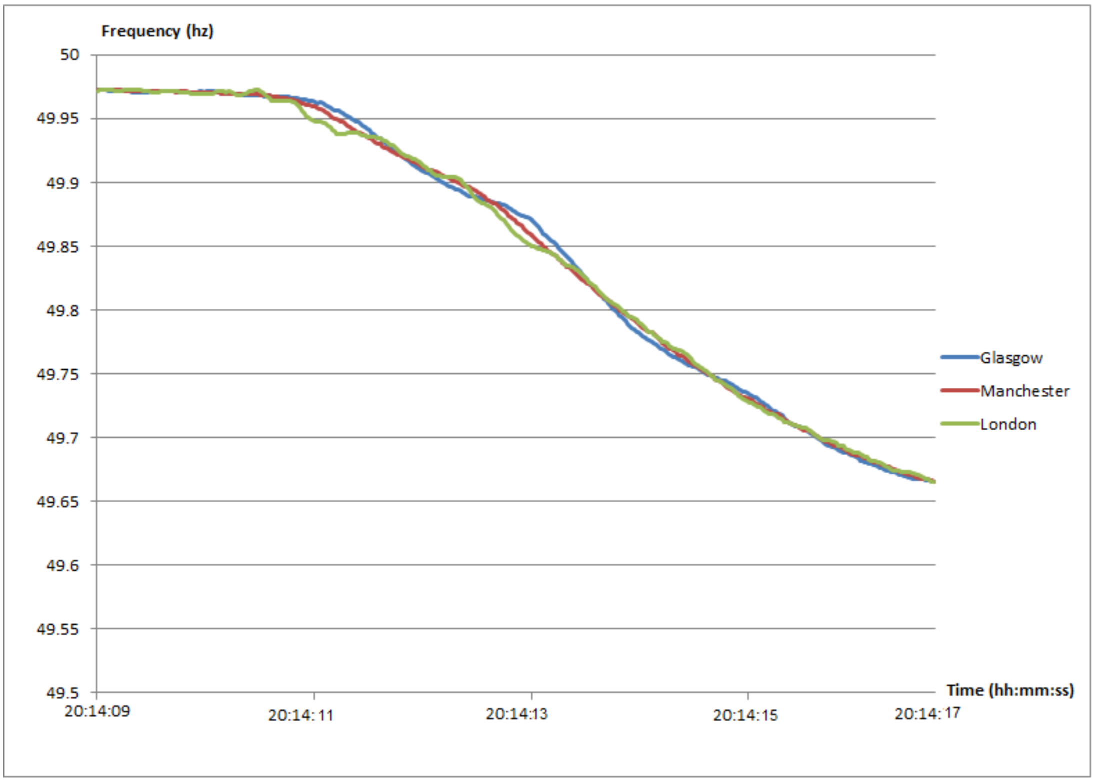

Figure 6.26. *Frequency traces during 1000MW Interconnector loss on 2 March 2012 [21]*

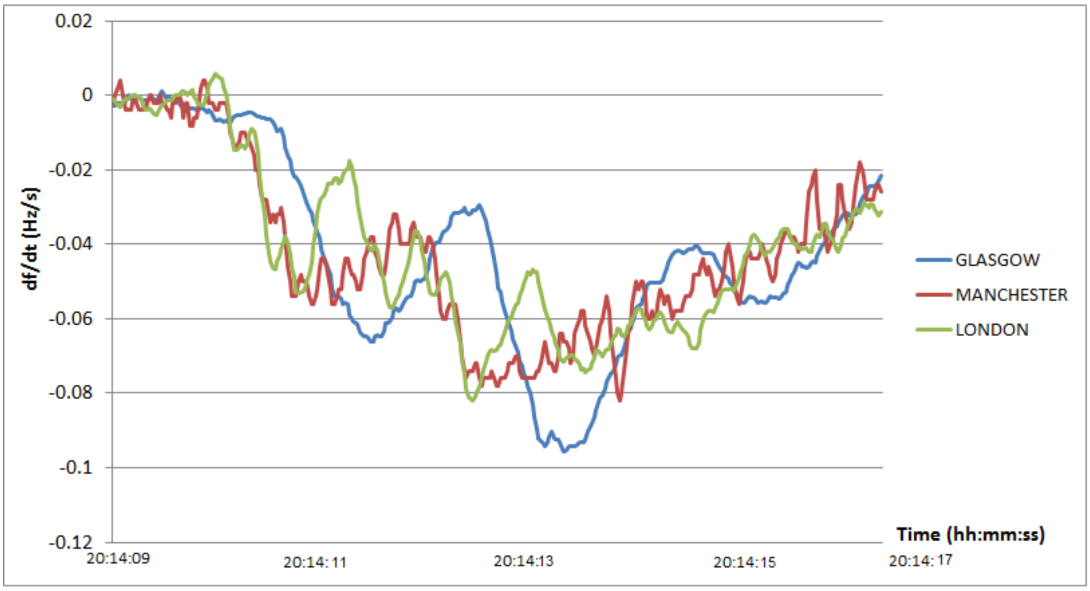

Figure 6.37. Average over 500 ms ROCOF of 1000MW Sizewell B loss in 2 March 2012

Based on these, it is assumed that any ROCOF events higher than the setting threshold will cause disconnection of the DGs due to ROCOF relays tripping at any part of the system. The amount of tripped DGs is based on number and capacities of DGs feed the network during the incident. Since there are difficulties in finding DG output data for the whole GB system for an entire year, it is assumed that the total DG output can be modelled using a triangular probability distribution. The minimum output is assumed 1 GW, the maximum output is 4 GW and the output with maximum probability is 2.5GW. The probability of 2.5GW output is

$$p(2.5) = \frac{2}{max - min} = \frac{2}{4-1} = 0.667 \tag{6.5}$$

The probability density function of the triangular distribution is shown in figure 6.28.

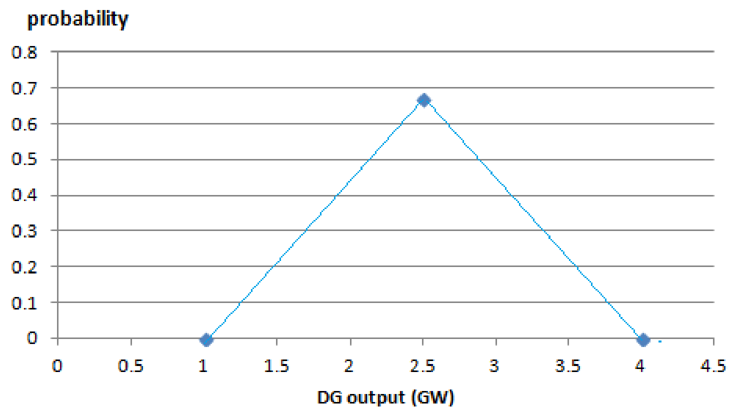

Figure 6.48. Density function of DG output in GB power system

Consequently, the probabilities of DG output range shown in table 6.16. are equal to the area under the graph of each interval. These probabilities are used as the input for node 'DGs trip?' of Bayesian Network risk model in figure 6.10.

Table 6.16. Probability of DG output

Output range (GW)	Probability
1 – 1.5	0.055
1.5 – 2.5	0.445
2.5 – 3.5	0.445
3.5 - 4	0.055

Based on the DIgSILENT simulation, the further frequency drop due to DGs trip can reach 48.8 Hz or lower. This causes demand under frequency protection trip [19]. The amount of demand disconnection is influenced by the frequency experienced in the system and the total demand during the incident. Demand disconnection can restore the frequency, but there are conditions that the system fails to recover and the stability may be lost. For this unstable condition, in this study, the system is assumed to suffer for blackout condition. The amount of disconnected demand is calculated based on under frequency protection setting in grid code as shown in table 6.17.

Table 6.17. Settings of Under Frequency Demand Disconnection in GB [22]

Frequency (Hz)	% demand disconnection for each network operator in transmission system		
	NGET	SPT	SHETL
48.8	5		
48.75	5		
48.7	10		
48.6	7.5		10
48.5	7.5	10	
48.4	7.5	10	10
48.3			
48.2	7.5	10	10
48.0	5	10	10
47.8	5		
Total % Demand	60	40	40

The percentage in table above are cumulative such that, should frequency fall to 48.6 Hz in the NGET Transmission Area, 27.5% of the total demand connected in the NGET Transmission Area shall be disconnected by the action of Low Frequency Relays.

An example of amount of demand disconnection for 20GW total demand is shown in table 6.18 for different total demand, wind level, large generation loss and DG disconnection. From the simulation result, the probability of demand interval disconnection is calculated. The result for 20GW demand and 0.3Hz/s setting no delay is shown in table 6.19. Similar calculation is carried out for other amount demands and settings then the probability results are assigned into the Bayesian Network CPT in node 'UF load shedding?' (figure 6.10).

Table 6.18. Demand disconnection (GW) due to under frequency protection trip

20GW demand	gen loss (MW)	demand disconnection for 1GW DG loss	demand disconnection for 2GW DG loss	demand disconnection for 3GW DG loss	demand disconnection for 4GW DG loss
High wind	1800	0.8984	3.5936	3.652528	5.5508
	1700	0.8984	1.7968	3.652528	5.1444
	1600	0.8984	1.7968	3.652528	4.9412
	1500	0.8984	3.5936	3.652528	blackout
	1400	0.8984	1.7968	3.5936	4.9412
	1320	0	1.7968	3.5936	3.652528
Medium wind	1800	1.7968	3.5936	5.000128	6.6952
	1700	1.7968	3.5936	5.000128	6.492
	1600	1.7968	3.5936	5.000128	6.6952
	1500	0	0	0	0
	1400	0	0	0	0
	1320	0	0	0	0

Table 6.19. Probability of demand disconnection for 20 GW demand due to DG trip for 0.3Hz/s setting no delay

Demand disconnection interval (GW)	20GW Demand			
	1 GW DG	2GW DG	3GW DG	4GW DG
no disconnection	0.111111	0	0	0
0.5 - 1.5	0.555556	0	0	0
1.55 - 2.5	0.333333	0.444444	0	0
2.55-3.5	0	0	0	0
3.55-4.5	0	0.555556	0.666667	0.11111
4.55-5.5	0	0	0.333333	0.33333
5.55-6.5	0	0	0	0.22222
6.55-7.5	0	0	0	0.22222
>7.55	0	0	0	0.11111

After updating the Bayesian network model (figure 6.10), the probability of demand disconnection due to applying ROCOF setting is shown in table 6.20 and 6.21. Also, the probability of DG capacity loss is shown in table 6.22

Table 6.20. Probability of unsupplied demand due to large generation loss for different ROCOF protection setting with no delay

Demand unsupplied (GW)	0.3 Hz/s	0.4Hz/s	0.5 Hz/s	0.6Hz/s	0.7Hz/s	0.8Hz/s	0.9Hz/s	1Hz/s
0	0.97783	0.98892	0.998966	1	1	1	1	1
0.5 - 1.5	0.00032	0.00028	0.000057	0	0	0	0	0
1.55 - 2.5	0.00250	0.00053	0.000230	0	0	0	0	0
2.55-3.5	0.00714	0.00275	0.000000	0	0	0	0	0
3.55-4.5	0.00469	0.00239	0.000690	0	0	0	0	0
4.55-5.5	0.00461	0.00290	0.000028	0	0	0	0	0
5.55-6.5	0.00257	0.00199	0.000028	0	0	0	0	0
6.55-7.5	0.00026	0.00023	0.000000	0	0	0	0	0
blackout	0.00007	0.00001	0.000000	0	0	0	0	0

Table 6.21. Probability of unsupplied demand due to large generation loss for different ROCOF protection setting with 500ms delay

Demand unsupplied (GW)	0.3 Hz/s	0.4Hz/s	0.5 Hz/s	0.6 Hz/s	0.7Hz/s	0.8Hz/s	0.9Hz/s	1Hz/s
0	0.988146	0.998967	1	1	1	1	1	1
0.5 - 1.5	0.000230	0.000057	0	0	0	0	0	0
1.55 - 2.5	0.000546	0.000276	0	0	0	0	0	0
2.55-3.5	0.002764	0.000000	0	0	0	0	0	0
3.55-4.5	0.002777	0.000644	0	0	0	0	0	0
4.55-5.5	0.002885	0.000038	0	0	0	0	0	0
5.55-6.5	0.002297	0.000019	0	0	0	0	0	0
6.55-7.5	0.000256	0.000000	0	0	0	0	0	0
blackout	0.000099	0.000000	0	0	0	0	0	0

Table 6.22. Probability of DG disconnection

DG (GW)	0.3 Hz/s	0.4Hz/s	0.5 Hz/s	0.6Hz/s	0.7Hz/s	0.8Hz/s	0.9Hz/s	1Hz/s
No delay								
1–1.5	0.001404	0.000616	5.69E-05	0	0	0	0	0
1.5–.5	0.011357	0.004982	0.000460	0	0	0	0	0
2.5-3.5	0.011357	0.004982	0.000460	0	0	0	0	0
3.5-4	0.001404	0.000616	5.69E-05	0	0	0	0	0
500ms delay								
1–1.5	0.000661	5.68E-05	0	0	0	0	0	0
1.5-2.5	0.005351	0.00046	0	0	0	0	0	0
2.5-3.5	0.005351	0.00046	0	0	0	0	0	0
3.5-4	0.000661	5.68E-05	0	0	0	0	0	0

The cost of unsupplied demand is based on value of loss load (VOLL) which according to London Economics [23] is £16,940/MWh. The average duration of demand disconnection is 43 to 63 minutes based on large generation loss incident at 27 may 2008 [22]. Taking the median 53 minutes as the average duration of demand disconnection, then the cost of each demand interval is shown in table 6.23. The costs are calculated as:

$$Cost_{demand} = VOLL \times demand \times hour \tag{6.6}$$

Where:

$VOLL$ = value of loss load in £/MWh =16,940

$demand$ = median of the demand interval in MW

$hour$ = average duration of demand disconnection in hour =53/60

Blackout is assumed as the total system disconnection. The blackout cost is calculated based on the average total demand for GB system i.e. 36.73GW.

Table 6.23. Demand disconnection cost

Interval of Demand loss (GW)	Cost for 53 minute demand disconnection (£)
0.5 - 1.5	14,963,667
1.55 - 2.5	29,927,333
2.55-3.5	44,891,000
3.55-4.5	59,854,667
4.55-5.5	74,818,333
5.55-6.5	89,782,000
6.55-7.5	104,745,667
blackout	549,615,477

DG disconnection costs consist of the loss of profit, DG shutdown-start-up cost and additional cost for utilisation of more expensive power from fast reserved generators. The profit of DG is £13.40/MWh, average shutdown-start-up cost is £19.94/MW capacity and additional cost of fast reserved utilisation is £22.87/MWh. Detail calculation of these DG disconnection costs can be found at appendix B.

If assumed DG disconnection duration is also 53 minutes then the cost of DG disconnection is:

$$Cost_{DG} = (profit + reserve) \times DG_{output} \times hour + cycling \times DG_{cap} \quad (6.7)$$

$$Cost_{DG} = (13.34 + 22.87) \times DG_{output} \times hour + 19.94 \times DG_{cap} \quad (6.8)$$

Where:

DG_{output} = DG output in MW

$hour$ = DG disconnection duration in hour = 53/60

$profit$ = profit from selling DG output (£/MWh)

$reserve$ = additional cost of fast reserved utilisation (£/MWh)

$cycling$ = shutdown-start up generator cost (£/MW)

DG_{cap} = capacity of disconnected DG which is assumed equal with output as usually DG operate at its rated capacity (MW)

Based on this equation, DG disconnection costs are shown in table 6.24.

Table 6.24. DG disconnection cost

DG loss (MW)	Length (minutes)	Cost of DG loss (£)
1000	53	51,976.53
2000	53	80,279.73
3000	53	120,419.60
4000	53	160,559.46

Using these costs times the probability of its occurrence, the risk in term of cost of unwanted ROCOF protection can be calculated. The risk in term of cost is discussed in section 6.8.

6.7.2. Consequences of unwanted operation due to nearby fault

Unwanted operation of ROCOF protection due to faults in the distribution network results in disconnection of the DG. The cost is the loss of DG profit, and shutdown-start-up cost for assumed disconnection duration of 1 hour. DG profit has been mentioned in section 6.7.1 i.e. £13.40/MWh while shutdown-start-up cost is £19.94/MWh. Therefore the average cost is £(13.40 + 19.94) times DG's average output (11.7MW) which is £390 for each DG unwanted operation.

6.7.3. Consequences of failure to operate

Based on results from [7], the durations of the balance between DG output and local demand vary from a few seconds to nearly 13 minutes which depends on ROCOF protection settings and load profile of each line. However, the islanding operation is restricted by the dead time of the autorecloser, which is assumed 20 seconds in the study. It is assumed that after out of synchronism of autorecloser operation, the DG cannot continue to operate due to DG damage or other protection operation (overcurrent protection for example). However, if the autorecloser recloses safely, there is a chance that islanding operation can sustain for another 20 seconds.

Therefore, the maximum duration of the islanding operation is assumed to be 40 seconds for the condition of DG output in balance with local demand for 40 seconds or more.

From the model of failure to operate risk in figure 6.8 there are two consequences of this failure mode: equipment damage and individual safety. Therefore the next sections are concerned with equipment damage impact and individual safety impact.

6.7.3.1. Equipment damage

The worst impact of the unsynchronized reclosure is severe damage of generator and prime mover due to high transient torque and damage of generator and transformer winding due to high current surge [24]. IEEE Standard 1547 provides specifications for safe DG synchronising as the differences of ±10 degree angle for capacity between 1.5MVA and 10MVA [25]. Beyond this limit, the equipment may suffer a level of damage. Most faulty damage happens for out of phase difference of 180 or 120 degree [26].

The air-gap torque magnitude caused by out of phase synchronization is shown in figure 6.29 [27]. For phase differences of more than 75 degree (rotor leading mains) the air-gap torque is higher than the three phase short circuit torque. If the plant is designed to withstand for three phase short circuit, then the damaging torque only happens for out of phase more than 75 degree but less than 150 degree. Similar graph for larger generator in [28] is shown in figure 6.30. The maximum torque that occurs between 110 to 130 degree phase differences (as in figure 6.30) is assumed as the torque which can cause 100% loss of generator, turbine and transformer life (called total damage). For phase differences between 75-150 degrees and excluding the range 110-130 degrees, the impact of out of phase synchronization is assumed result in 50% damage.

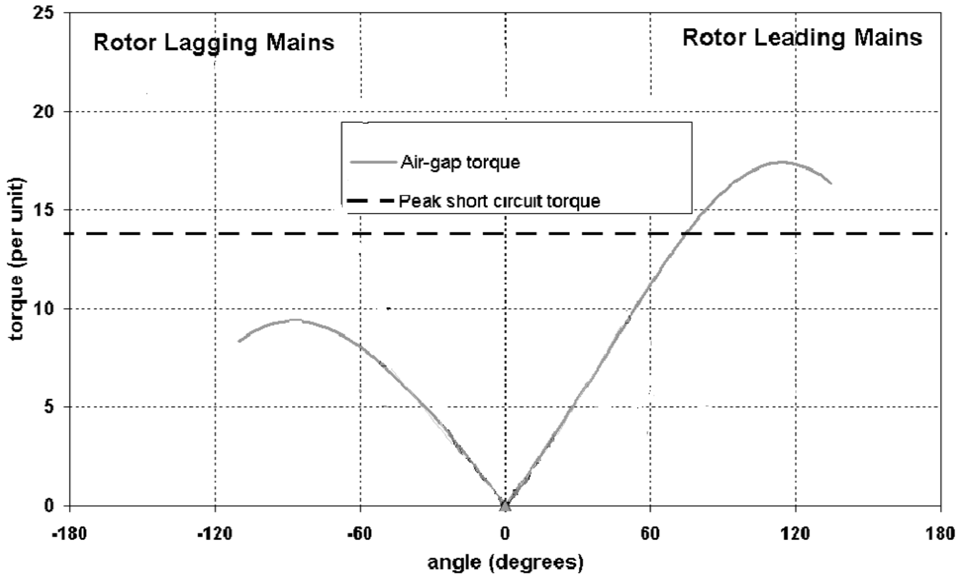

Figure 6.59. Torque caused by out of phase synchronization [27]

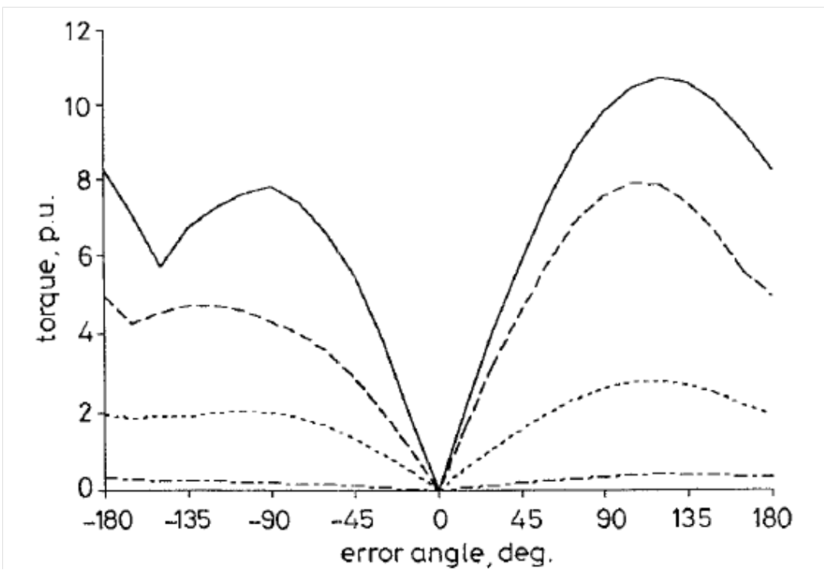

Figure 6.30. Torque caused by out of phase synchronization for larger generator [28]

The probability occurrence of any degree of phase difference is assumed to have uniform distribution. Therefore the probability of 110-130 degree phase difference is:

$$(130 - 110)/360 = 0.055556$$

and the probability for 130-180 or 75-110 degree is:

$$[(150-130)+(110-75)]/360=0.1528$$

This leaves the probability of safe autoreclosing (with no check synchronous applied) as:

$$1-0.05556-0.1528=0.79167$$

The autorecloser can reconnect the network successfully in ±10 degree angle difference with the probability (2x10)/360 = 0.055556. However, the second attempt to reclose may cause total damage for the equipment with the probability:

$$P(\pm 10°) \times P(110°\text{-}130°) = 0.055556 \times 0.055556 = 0.003086$$

and 50% damage with probability:

$$P(\pm 10°) \times P(130°\text{-}150° \cup 75°\text{-}110°) = 0.055556 \times 0.1528 = 0.008489$$

Therefore, these values can be used for CPT of node ‘Damage of electrical equipment in the network’ of the Bayesian network model in figure 6.4 as shown in figure 6.27. From figure 6.27 can be seen that probability of ‘damage50’ and ‘totaldamage’ during protection in ‘fail’ state and out-synchronism reclosure in ‘norisk’ state are based on probability of damage after second reclose given the first reclose is successful.

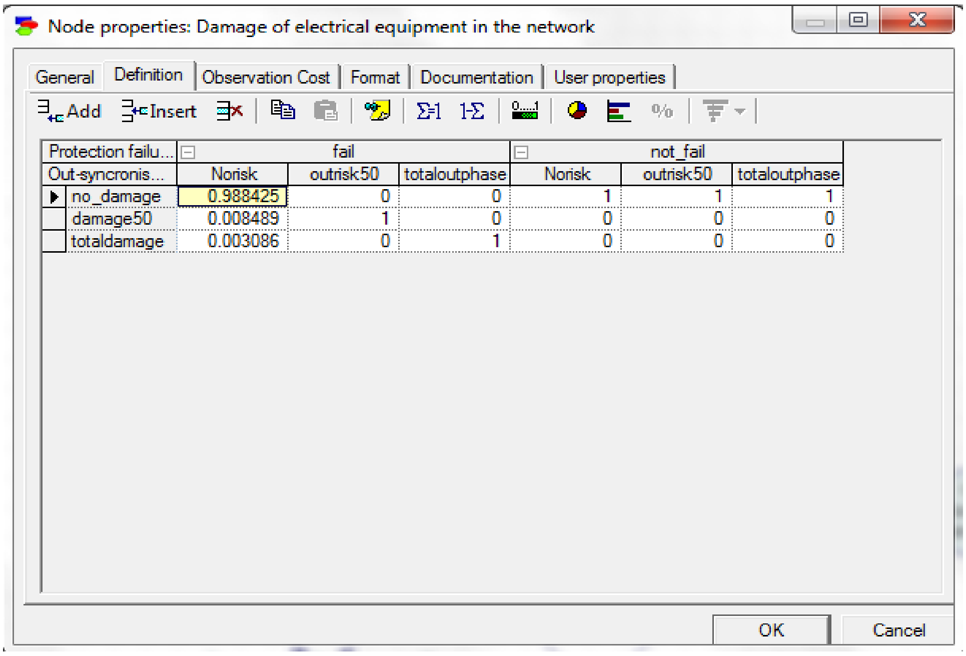

Figure 6.31. CPT of Node 'Damage of electrical equipment in the network'

The calculated probability of the damages for different ROCOF protection settings from the Bayesian Network model is shown in table 6.25. It can be seen that higher Hz/s setting results in higher probability of damages and introducing delay causes more damage probability.

Table 6.25. Probability of equipment damage

Setting	Setting no delay		Setting 500ms delay	
	50% damage	Total damage	50% damage	Total damage
0.3	6.08E-05	2.210E-05	1.19E-04	4.325E-05
0.4	9.669E-05	3.516E-05	1.584E-04	5.759E-05
0.5	1.312E-04	4.770E-05	1.98E-04	7.199E-05
0.6	1.783E-04	6.484E-05	2.372E-04	8.627E-05
0.7	2.211E-04	8.040E-05	2.767E-04	1.006E-04
0.8	2.638E-04	9.592E-05	3.161E-04	1.150E-04
0.9	3.049E-04	1.109E-04	3.556E-04	1.293E-04
1	3.445E-04	1.25E-04	3.950E-04	1.44E-04

The cost of equipment damage is calculated in terms of the current book value or net asset value of the generator, turbine and step-up transformer for the total damage and 50% of the current book value for 50% damage. Book value of an asset is the original cost of the asset minus accumulated depreciation. The capital cost of generator, turbine and step-up transformer for DG with capacity 11.7MW is £3,959,355 [29,30] with an assumed economic lifetime of 20 years. By assuming the damage occurs at 5 years operation (a quarter of lifetime) with depreciation 3.4% per year [31], the net asset value at year 5 is £3,286,265 for total damage and assumed half of it i.e. £1,979,678 for 50% damages. In addition to the equipment damage, the consequence of the protection failure to operate is including loss of profit that the DG should earn. The profit loss can be calculated as

$$profitloss_{damage} = profit \times DG_{output} \times hour \times LF \tag{6.9}$$

Where

$profit$ = profit that the DG should earn (£/MWh)

DG_{output} = output of DG (MW)

$hour$ = duration of DG outage (hour, assume 1 year for total damage and 6 months for 50% damage)

LF = average load factor of GB's DG = 0.589538368 (in appendix C).

Equation (6.9) gives the cost of £4,096,566 for total damage and £2,048,283 for 50% damage for the average DG capacity 11.7MW and the average loading factor 0.5895.

6.7.3.2. Individual safety

Fatality caused by the unintended islanding of DG operation is calculated using the Bayesian Network of Figure 6.8. The probability of an electrical worker to be in close proximity of HV islanding network is calculated as:

$$P_{vicinity} = \frac{duration\ of\ work\ in\ the\ HV\ network\ for\ a\ year\ (minutes)}{time\ in\ a\ year\ (minutes)} \tag{6.10}$$

Duration of work in HV network for a year is total duration of repair and maintenance work in the HV distribution network of a typical islanding network, for this study this is assumed to be a 33 kV network with five distribution substations.

As the average minute of loss supply per GB customer for HV distribution network faults is 70 minutes/year/customer [32] and number of total GB customer is 29,687,000 [30] then total duration of loss of supply is

$$70 \times 29{,}687{,}000 = 2{,}078{,}090{,}000 \text{ minutes/year.}$$

Since the number of fault experienced in GB HV distribution network is 180385 fault/year [32], then average outage duration is

$$2{,}078{,}090{,}000/180385 = 11520.3 \text{ minutes/fault.}$$

The probability of a customer experiencing a distribution fault is 0.7 fault/year [32]. If assume that probability of fault occurrence in the islanding network is twice of the probability of a customer experienced a distribution fault, the duration of outage in the islanding network is

$$2 \times 0.7 \times 11520.3 = 16128.4 \text{ minutes/year.}$$

This duration is taken as average duration of repair work in a year in an islanding network.

Maintenance duration is calculated based on frequency of inspection and maintenance for every equipment in HV distribution network in [34]. Duration for each maintenance work is assumed and the number of equipment is based on HV distribution network with five distribution substation. Details of calculation are shown in appendix B. The calculated duration of the maintenance work is 19311.7 minutes/year.

Adding the maintenance duration/year with the duration of repair work/year, the total duration of worker in vicinity of a HV islanded network is 35440.1minutes/year. Then using the equation (6.10) the probability of worker in close proximity of HV network is 0.0674.

According to [35], the average of fatality in GB network is 8.6 worker/year with 90% of them involving HV network. The total number of HV worker in vicinity of the network proximity per year is 800 workers. This gave the annual probability of a worker in proximity faulted HV network being killed: (8.6 x 90%)/800 = 0.01. As the maximum islanding duration is only around 40 seconds, hence the probability of worker in proximity being killed is 0.01x40/(365x24x60x60)= 1.2 x 10^{-8}.

Using 1.2 x 10^{-8}as the probability of 'maintenance personnel touches bare conductor' (and being killed) and 0.0674 as the probability of 'electrical workers in vicinity HV network' then the updating of Bayesian Network in figure 6.8 gives a probability of fatality of 8.3687632x10^{-13} for 0.5Hz/s 500ms delay setting. This fatality probability is in the range of the broadly acceptable region in the HSE framework of individual risk (less than 10^{-6}). Fatality probabilities for different settings are shown in table 6.26. From the table can be seen that all settings results in broadly acceptable fatality risk.

Table 6.26. Fatality probability of ROCOF protection settings

Setting (Hz/s)	Setting no delay	Setting 500ms delay
0.3	2.5693685 x 10^{-13}	5.0277604 x 10^{-13}
0.4	4.0874939 x 10^{-13}	6.6950106 x 10^{-13}
0.5	5.5450372 x 10^{-13}	8.3687632 x 10^{-13}
0.6	7.5386062 x 10^{-13}	1.0029511 x 10^{-12}
0.7	9.3467445 x 10^{-13}	1.1696761 x 10^{-12}
0.8	1.1151848 x 10^{-12}	1.3364011 x 10^{-12}
0.9	1.2891493 x 10^{-12}	1.5031261 x 10^{-12}
1	1.456568 x 10^{-12}	1.6698511 x 10^{-12}

6.8. Risk of failure modes

Risk is the product of probability occurrence of the undesired event and its impact. In this study the impact is considered as cost and individual safety.

6.8.1. Risk of unwanted operation due to large generation loss

Section 6.7.1 has shown the impact of unwanted operation due to large generation loss. Large amount of demand disconnection can cause serious implication for customer. This study only considers the direct cost of demand disconnection, as the indirect cost of large demand disconnection is difficult to calculate. The indirect cost is including social and political cost [36].

Risk of unwanted operation due to large generation loss is calculated as follow:

$$R_g = R_d + R_{DG} \tag{6.11}$$

$$R_d = \sum_{i}^{n} P_{d\,i} \times C_{d\,i} \tag{6.12}$$

$$R_{DG} = \sum_{j}^{m} P_{DG\,j} \times C_{DG\,j} \tag{6.13}$$

Where:

R_g = Risk of unwanted operation due to large generation loss

R_d = Risk from demand disconnection

R_{DG} = Risk from DG disconnection

$P_{d\,i}$ = probability of demand disconnection interval due to large generation loss

$C_{d\,i}$ = Cost of demand disconnection interval

n = number of demand interval

$P_{DG\,j}$ = probability of disconnection of DG capacity interval due to large generation loss

$C_{DG\,j}$ = profit loss from DG output interval

m = number of DG output interval

Multiplication of demand disconnection cost in table 6.23 to the probability of demand disconnection in table 6.20 and 6.21 give risk of demand disconnection. Also, multiplication of the probability DG disconnection in table 6.22 and the DG disconnection cost in table 6.24 give the risk of DG disconnection. As a result, total risk of unwanted operation of ROCOF protection is shown in table 6.27.

Table 6.27. Risk of unwanted operation due to large generation loss for each setting

Setting	Risk (£)/year	
	No delay	500 ms delay
0.3	1326490.04	814447.20
0.4	713375.91	52265.76
0.5	53849.75	0
0.6	0	0
0.7	0	0
0.8	0	0
0.9	0	0
1	0	0

6.8.2. Risk of unwanted operation due to nearby fault

Risk of unwanted operation due to nearby fault is calculated by multiplying the frequency of its occurrence (in table 6.10) with the impact cost. The risk result for each DG is shown in table 6.28.

Table 6.28. Risk of unwanted operation due to nearby fault for one DG

Setting	Risk (£)/year	
	No delay	500ms delay
0.3	2,225.34	2,174.87
0.4	2,225.34	2,041.60
0.5	2,174.87	1,823.68
0.6	2,076.37	1,691.64
0.7	2,013.28	1,575.54
0.8	1,879.77	1,530.11
0.9	1,829.53	1,387.48
1	1,779.06	1,246.40

Since 342 DGs having ROCOF protection is predicted for year 2020 (as calculated in appendix C) the risk of unwanted operation due to nearby fault for total GB is multiplication of each risk in table 6.28 to 342 as shown in table 6.29.

Table 6.29. Total GB risk of unwanted operation due to nearby faul

Setting	Total GB Risk (£)/year	
	No delay	500ms delay
0.3	761,066.73	743,805.04
0.4	761,066.73	698,228.75
0.5	743,805.04	623,698.24
0.6	710,117.50	578,539.85
0.7	688,540.39	538,833.96
0.8	642,879.90	523,297.21
0.9	625,699.32	474,519.01
1	608,437.64	426,269.57

6.8.3. Risk of failure to operate

From the previous section, the individual safety risk of ROCOF protection falls in the broadly acceptable region for all setting considered in the assessment (up to 1Hz/s with 500ms delay).

Risk from equipment damage is product of its occurrence probability in table 6.25 to the cost of the damage which is £4,096,566 for total damage and £2,048,283 for 50% damage. The risk result is shown in table 6.30 which is based on one unit DG. For total DG with ROCOF protection in GB (342 unit), the result is shown in table 6.31. From these results, it can be seen that the risk increases with setting increase and applied delay.

Table 6.30. Risk of failure to operate of a ROCOF protection

Setting	Risk (£)/year	
	No delay	500ms delay
0.3	215.03	420.77
0.4	342.08	560.30
0.5	464.06	700.37
0.6	630.90	839.36
0.7	782.22	978.89
0.8	933.28	1118.42
0.9	1078.87	1257.95
1	1218.98	1397.48

Table 6.31. Total GB risk of failure to operate of ROCOF protection

Setting	Risk (£)/year	
	No delay	500ms delay
0.3	73539.21	143902.10
0.4	116990.25	191621.31
0.5	158707.34	239526.64
0.6	215766.29	287059.74
0.7	267517.94	334778.96
0.8	319182.74	382498.18
0.9	368974.01	430217.39
1	416891.75	477936.61

6.9. Optimum setting

The optimum setting is defined as the setting which gives minimum total risk. The total risk is calculated as:

$$R_T = \sum_{i=1}^{n} R_i \tag{6.14}$$

Where:
R_T = Total risk
R_i = risk of failure mode i
n = number of failure mode = 3

The calculated total risks of DGs in GB are shown in table 6.32 and figure 6.32. Figure 6.32 also shows each failure mode risk for 500ms delay setting. The total risk for both time settings are shown in figure 6.33 which indicates that the minimum risk is achieved for setting 0.5Hz/s with 500ms delay, hence it will be the chosen optimum setting.

Table 6.32. Total GB annual risk of ROCOF protection

Setting (Hz/s)	No delay	500ms delay
0.3	2161096	1702154
0.4	1591433	942116
0.5	956362	863225
0.6	925884	865600
0.7	956058	873613
0.8	962063	905795
0.9	994673	904736
1	1025329	904206

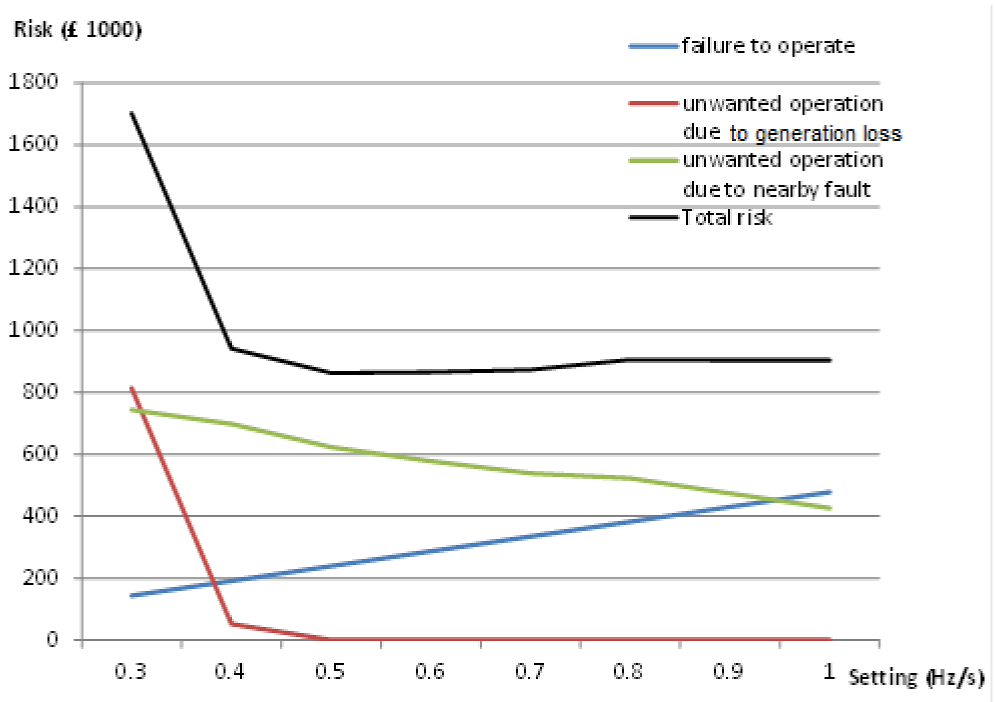

Figure 6.32. Risk of failure modes for 500ms delay setting

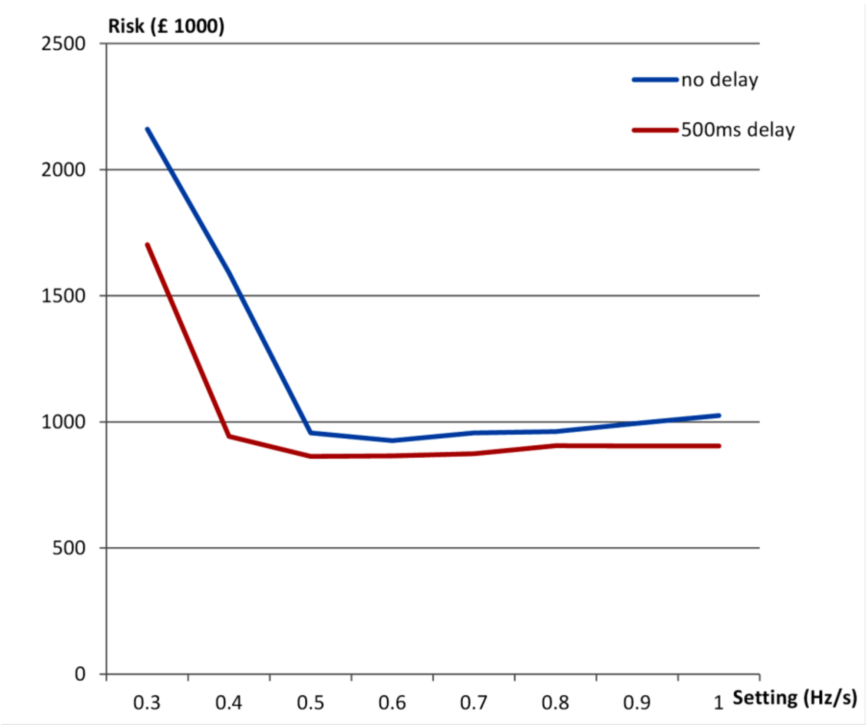

Figure 6.33. Risk of ROCOF protection in the GB system

6.10. Sensitivity analysis

Sensitivity analysis aims to find out the effect of data variation on the risk result and the optimum settings. Some data which is based on assumption will be examined with sensitivity analysis. The data includes local load profile compared to DG output, cost of cascading failure and cost of equipment damage. The optimum setting obtained for the based case will then be compared to the results from sensitivity analysis.

6.10.1. Local load profile

The risk for failure to operate highly depends on the recorded load profile data. The variation of load profile in the distribution networks is unlimited. The base case results in table 6.32 are based on average of three load profile in [7]. Sensitivity analysis for the worst case of load profile which causes the highest probability of failure to operate, results in the same optimum setting i.e. 0.5 Hz/s with 500 ms delay as shown in figure 6.34. For the same setting, the risk magnitude for the worst case load profile (figure 6.34) is higher than the base case (figure 6.33). This is due to the increase of failure to operate risk in the worst case load profile. In order to compensate the effect of worst case load profile upon the risk magnitude, logically the setting should be decreased, because a low setting is preferred to prevent failure to operate. However, at low settings (less than 0.5 Hz/s), the risk from unwanted operation due to large generation loss is extremely high and this diminishes the reduction of failure to operate risk. Therefore, the optimal setting remains the same.

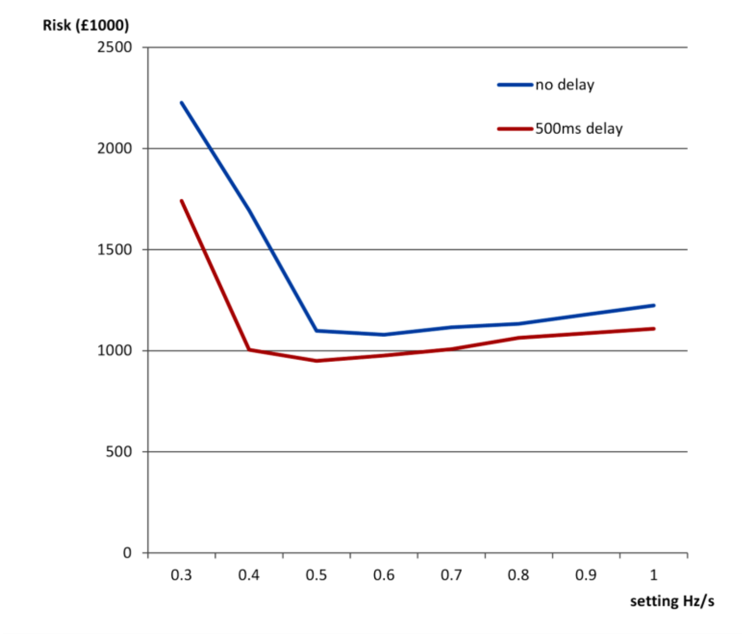

Figure 6.64. Risk of ROCOF protection in GB for the worst case load profile

However there is the possibility that not all DG can balance its output with the local demand. If it is assumed that only 50% of DG can balance its output with local demand, the risk from failure to operate will reduce. Therefore using the base case load profile and having 50% of DG output in balance with local demand give the total GB risk as shown in figure 6.35 and the optimum setting is 1Hz/s with 500ms delay. The increasing of the optimum setting reflects more dominant impact of unwanted operation due to nearby fault with reducing risk of failure to operate.

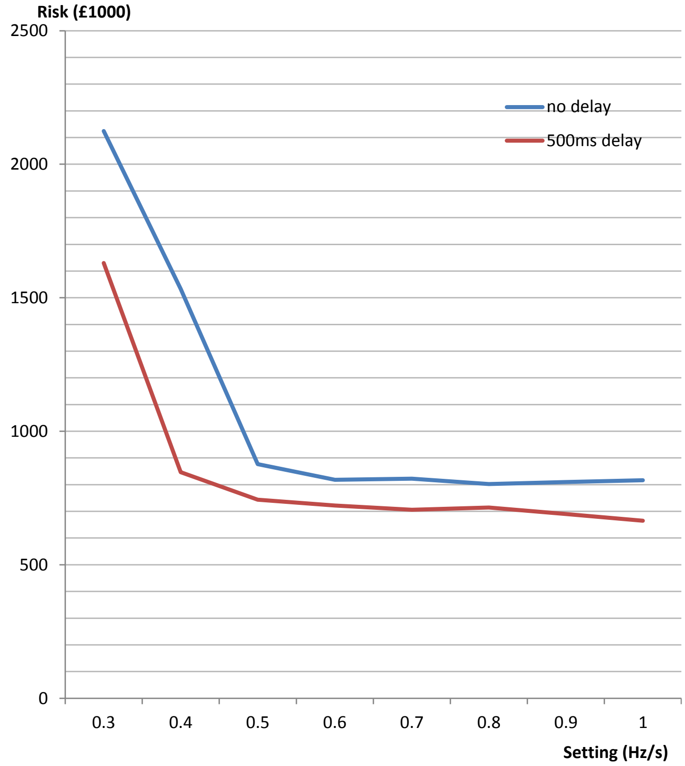

Figure 6.35. Risk index of ROCOF protection for 50% less DGs can balance with local demand

6.10.2. Cost of cascading failure

In the base case, the cost of cascading failure due to large generation loss is only considered as a direct cost because of difficulty in calculating the indirect cost. Assuming that indirect cost is a percentage of direct cost, then the sensitivity analysis will discover its impact to the optimum setting. The results show in table 6.33. It is found that the optimum setting remains the same for any increase of indirect cost. It is because for setting at 0.5Hz/s or higher (500ms delay) or 0.6Hz/s or higher (no delay) the probability of unwanted operation is zero. Therefore any increase of its impact cost do not affect the risk of these high settings, while lower setting causes less risk of failure to operate hence the risk due to large generation loss become more dominant.

Table 6.33. Optimum setting for percentage of indirect cost to direct cost

Percentage of indirect cost	Optimum setting
50	0.5Hz/s 500ms delay
60	0.5Hz/s 500ms delay
70	0.5Hz/s 500ms delay
80	0.5Hz/s 500ms delay
90	0.5Hz/s 500ms delay
100	0.5Hz/s 500ms delay
200	0.5Hz/s 500ms delay
300	0.5Hz/s 500ms delay

6.10.3. Cost of equipment damage

The cost of equipment damage is related to the purchase price of the equipment, depreciation rate and age of the equipment when the damage occurs. The base case assumes a depreciation rate 3.4% [31] and age of the equipment as 5 years old. However, the price of electrical equipment (turbine, generator and transformer) tends to increase every year [37], the age of equipment when the damage occurs varies as well as the depreciation rate. Therefore, sensitivity analysis is carried out for the cost of equipment damage. The cost is varied from lower to higher than the base case. The result is shown in table 6.34.

Table 6.34. Optimum setting for different equipment damage cost

Percentage of equipment damage cost to based case (%)	Optimum setting
50	1Hz/s 500ms delay
80	0.6Hz/s 500ms delay
100 (base case)	0.5Hz/s 500ms delay
120	0.5Hz/s 500ms delay
150	0.5Hz/s 500ms delay
180	0.5Hz/s 500ms delay
200	0.5Hz/s 500ms delay

The result in table 6.34 shows for the equipment damage cost less than base case, the optimum setting is higher than 0.5Hz/s but when the cost is higher than the base case the optimum setting is 0.5Hz/s. This shows that equipment damage cost is a sensitive variable in choosing the optimum settings. However as already mentioned, the equipment cost tends to increase, hence the chosen optimum setting 0.5Hz/s with 500ms delay can cover this tendency.

6.11. Chapter Summary

Trade-off between the risk of failure to operate and unwanted operation of ROCOF protection has been investigated in order to find the optimal setting for this type of protection. From the risk assessment study, the optimum setting of ROCOF protection in Great Britain in year 2020 is 0.5Hz/s with 500ms delay which gives the minimum level of risk. The study also considers some variation of the assumed data in order to find any effects on the optimum setting. In general, the optimum setting remains the same because of the dominant risk magnitude from unwanted operations due to large generation loss for low settings and it becomes zero for settings higher than 0.5 Hz/s. Since, the risk of failure to operate rises in parallel with the increasing of the settings, the minimum risk is achieved when the risk from unwanted operation due to large generation loss tends to zero and the risk from failure to operate is still relatively small i.e. at a setting of 0.5 Hz/s. If only 50% of the number of DG with ROCOF protection in GB power system can have output equal to local demand, then the risk from failure to operate will be reduced. Therefore, the trade-off will be influenced by failure to operate and unwanted operation due to nearby faults mode. This condition gives the optimum setting at 1Hz/s with a 500ms delay. The optimal settings are within the broadly acceptable region of individual safety.

6.12. References for Chapter 6

[1] D. Toke, "The UK offshore wind power programme: A sea-change in UK energy policy?," *Energy Policy,* vol. 39, pp. 526-534, 2011.

[2] National-Grid, "Future Frequency Response Services," National grid2010.

[3] A. Dyśko, C. Booth, O. Anaya-Lara, and G. M. Burt, "Reducing unnecessary disconnection of renewable generation from the power system," *IET Renewable Power Generation,* vol. 1, pp. 41-48, 2007.

[4] *The Distribution Code and The Guide to the Distribution Code,*. Great Britain Issue 20, 2013.

[5] National-Grid, "GC022 - Frequency Response," National grid, United Kingdom2013.

[6] C. Foote. UKGDS EHV1 [Online]. Available: https://www.dropbox.com/s/e5pu0gkaxzyq17h/UKGDS_WebSiteContent.zip

[7] A. Dysko, I. Abdulhadi, X. Li, and C. Booth, "Assessment of Risk Resulting from the Adjustment of ROCOF Based Loss of Mains Protection Settings, Phase I " University of Strathclyde, Glasgow2013. available at : http://www2.nationalgrid.com/UK/Industry-information/Electricity-codes/Grid-code/Modifications/GC0035-GC0079/

[8] National-Grid, "Frequency Changes during Large Disturbances and their Impact on the Total System," National Grid, London2013.

[9] DIgSILENT_Technical_Documentation, "What's New in Power Factory Version 14.1," ed. Gomaringen: DIgSILENT GmbH, 2011.

[10] *Recomendation for the Connection of Generating Plant to the Distribution Systems of Licensed Distribution Network Operators*, ENA G59, 2010.

[11] M. H. Bollen and F. Hassan, *Integration of distributed generation in the power system* vol. 80: John Wiley & Sons, 2011.

[12] NETS_SQSS, "Offshore Infeed Loss Working Group (GSR013)," National Grid, United Kingdom2012.

[13] National-Grid, "TEC Register - 22 January 2014," T. R.-J. 2014, Ed., ed. London: National_Grid, 2014.

[14] *IAEA Safety Standart Series, Safety of Nuclear Power Plant: Design*, IAEA, 2000.

[15] NETS_SQSS, "Transmission Entry Working Group," National Grid, 2012.

[16] G. Sinden, "Characteristics of the UK wind resource: Long-term patterns and relationship to electricity demand," *Energy Policy*, vol. 35, pp. 112-127, 2007.

[17] National_Grid, "UK Future Energy Scenario," National Grid, London2013.

[18] I. S. Ilie, I. Hernando-Gil, and S. Z. Djokic, "Reliability equivalents of LV and MV distribution networks," in *Energy Conference and Exhibition (ENERGYCON), 2012 IEEE International*, 2012, pp. 343-348.

[19] National_Grid, "Electricity Ten Year Statement," National Grid, London2012.

[20] National_Grid, "Annual Summary Report for Significant System Events (1 August 2011 to 31 July 2012)," National Grid, London2012.

[21] GB power system PMU, Department Electronic and Electrical Engineering, University of Strathclyde. contact: Dr Adam Dysko: a.dysko@strath.ac.uk

[22] National_Grid, "Report of the National Grid Investigation into the Frequency Deviation and Automatic Demand Disconnection that Occured on the 27 May 2008," London2009.

[23] London-Economics, "The Value of Lost Load (VoLL) for Electricity in Great Britain. Final report for OFGEM and DECC," London Economics, London2013.

[24] M. J. Thompson, "Fundamentals and advancements in generator synchronizing systems," in *Protective Relay Engineers, 2012 65th Annual Conference for*, 2012, pp. 203-214.

[25] "IEEE Application Guide for IEEE Std 1547(TM), IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems," *IEEE Std 1547.2-2008*, pp. 1-217, 2009.

[26] "IEEE Standard for Salient-Pole 50 Hz and 60 Hz Synchronous Generators and Generator/Motors for Hydraulic Turbine Applications Rated 5 MVA and Above," *IEEE Std C50.12-2005 (Previously designated as ANSI C50.12-1982)*, pp. 1-45, 2006.

[27] R. J. Best, D. J. Morrow, and P. A. Crossley, "Out-of-Phase Synchronization of a Small Alternator," in *Power Engineering Society General Meeting, 2007. IEEE*, 2007, pp. 1-7.

[28] S. O. Faried, R. Billinton, S. Aboreshaid, and M. Fotuhi-Firuzabad, "Stochastic evaluation of turbine-generator shaft torsional torques during faulty synchronisation," *Generation, Transmission and Distribution, IEE Proceedings-*, vol. 143, pp. 487-491, 1996.

[29] Mott_MacDonald, "UK Electricity Generation Cost Update," Mott MacDonald, Brighton2010.

[30] Available: http://electrical-engineering-portal.com/an-overview-of-large-power-transformer-lpt

[31] ICRA-Advisory-Services, "Discussion on Depreciation Norms," ICRA Limited2000.

[32] Ofgem, "Electricity Distribution Annual Report for 2010-11," Ofgem2012.

[33] M. Gregory, S. Khan, and S. Stadnyk, "Sub-national Electricity Consumption Statistics. Regional and Local Authority Level Statistics (2012 Data)," D. o. E. C. Change, Ed., ed. London, 2013.

[34] Powerco, "Our Assets. Asset Management Plant 2013," Powerco, New Plymouth2013.

[35] DCRP-G59-Working-Group, "Embedded generation interface protection: Assessment of risks arising from relaxation in the application of neutral voltage displacement (NVD) interface protection," December 2009.

[36] H. Brayley, M. A. Redfern, and Z. Q. Bo, "The Public Perception of Power Blackouts," in *Transmission and Distribution Conference and Exhibition: Asia and Pacific, 2005 IEEE/PES*, 2005, pp. 1-5.

[37] U.S.-Energy-Information-Administration, "Updated Capital Cost Estimates for Utility Scale Electricity Generating Plants," U.S. Department of Energy, Washington2013.

Chapter 7. Case Study: Adaptive Overcurrent Protection

This case study presents implementation of the risk assessment framework to select the optimum power system protection option for a given distribution network incorporating DGs. The protection candidate is an adaptive overcurrent protection scheme compared to non-adaptive traditional protection. The case study is based on a proposed protection scheme in an IEEE publication [1]. The assumptions, which are applied for the case study, have simplified the scope of the assessment. The assessment reveals the risk of applying the proposed protection candidate which is compared to the conventional overcurrent scheme. Therefore, it can assist in the decision making process for protection schemes.

7.1. Introduction

Distributed generation is prevented to operate in islanded network, following a loss of main event. One of the reasons is the inability of the existing system protection on the network to cope with different magnitudes and directions of current during islanding. However, as DGs supplying islanded network can improve system reliability, new schemes of protection which consider grid connected and islanded conditions can support in realising the full benefit of DG. One of the protection schemes, *simple adaptive overcurrent protection of distribution systems with distributed generation* [1], is proposed as a protection candidate for the given distribution network. The adaptive protection changes its setting to align with the changes of primary system states.

Applying adaptive functionality for a protection scheme introduces additional risks. The risks might come from failures to detect primary system states correctly, delays in implementing setting changes or an inherent failure of the adaptive protection functionality. This additional uncertainty can cause unintended deterioration of protection performance (compared to conventional protection) if not managed appropriately. Therefore, the proposed protection scheme should be assessed to make sure that the risk level is acceptable.

7.2. The adaptive overcurrent protection scheme

This section will explain the adaptive protection scheme and the protected primary system [1] in order to demonstrate how the overall scheme functions. The primary system is an underground distribution network as shown in figure 7.1. The adaptive protections are the directional over current protection for the distribution lines which have prefix P in figure 7.1. Data associated with the system can be found in appendix D.

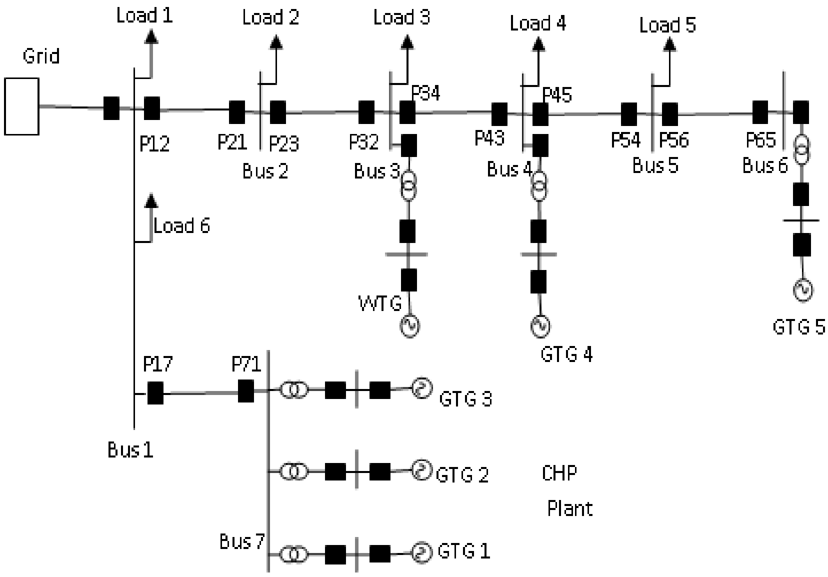

Figure 7.1. Single line diagram of the distribution network which protected by the adaptive overcurrent protection [1] © 2011 IEEE

The network can operate in states of grid connected or disconnected and all DG connected or the DG(s) disconnected. Therefore, the protection may needs adaptive functionality in order to operate correctly under the changes of network conditions

There are two directional over current relays located at either end of each line. The protection which looks downstream (forward looking protection) is designed to operate either in grid connected or islanded state. The protection which looks upstream (reverse looking protection) is designed to operate when all DGs are connected and when one or more DG(s) at downstream are disconnected.

The fault current seen by the forward looking protection (P12, P23, P34, P45 and P56) during islanding is lower than during grid connected mode. Although using the grid connected settings during islanding state, the protection still able to clear faults in their protected area; however the time to clear the faults will be longer hence it can cause tripping of Wind Turbine Generation (WTG) interface protection. Therefore this protection needs two setting groups: for the grid connected state and for the islanded state.

If any DGs on the downstream network are disconnected, the reverse looking protection (P21, P32 and P43) will see lower fault current magnitude than normal condition (i.e. all DGs connected). Therefore, this protection also needs more than one setting group: normal state and DG(s) disconnection. Only GTG 5 disconnection state is applied in [1] to demonstrate the protection scheme.

The adaptive protections have two directional over current tripping characteristics: instantaneous and IDMT. Instantaneous trip is preferable to avoid the loss of the WTG due to the WTG's under voltage protection trip. Fault ride through capability, which is based on Danish grid code in [1], is shown in figure 5.2. The instantaneous settings are based on bolted fault current near the end of the lines.

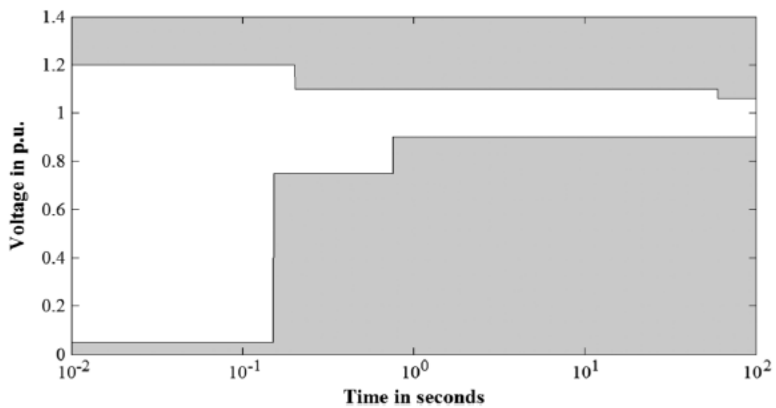

Figure 7.2. Fault ride through for wind turbines [1] © 2011 IEEE

The adaptive protection changes its settings based on the detected system state. Three state detection techniques are applied to the protection system: an islanding detection, a grid reconnected detection and loss of DG detection. Islanding and grid reconnected detection uses a hybrid technique which combines passive and active detection [2], [3]. Passive detection is based on a measured power system quantity to detect the system states. However, as for some circumstances the measurement result cannot distinguish the system states, hence active detection of islanding or grid reconnected needs to be applied.

The hybrid detection systems are located near CHP units to allow its active algorithm to increase or decrease the CHP power output. A passive islanding and grid reconnected detection are also placed at each forward protection relay so that system state information is provided for the relay directly. Both detection algorithms are detailed in [1]. Based on the system state information, the relay will adjust its setting group.

The last detection method, loss of DG detection is measured by upstream relays when a DG is disconnected from the network due to circuit breaker operation to clear a fault. The detection is based on the clearing time and current magnitude of a downstream fault and stored time-overcurrent characteristics of every downstream relays [1]. This detection algorithm is embedded in the overcurrent relay hence no additional equipment is needed. The three detection techniques work based on the local information only, therefore, no dedicated communications are required to provide the adaptive functionality of the protection schemes.

In the scheme, only lines 12, 23 and 34 have both adaptive forward and adaptive reverse schemes. Moreover, reference [1] only provides two setting groups for the adaptive reverse looking scheme, i.e. for normal and GTG5 disconnection states. Therefore, for the purposes of this case study, protection on line 34 (P34 and P43) is chosen to be the assessed adaptive protection in term of risk. Since the adaptive protection is designed for three phase faults [1], all the faults on the line 34 in the rest of the paragraph are indicated three phase faults.

7.3. Assumptions, data and scenario in the study

In order to simplify and make the risk assessment possible to be carried out, this study is based on several assumptions i.e.:

a) The hybrid islanding and grid reconnected detection do not have non-detection zone
b) no external system events are incorrectly detected as islanding or grid-reconnected events
c) Backup protection is assumed operating correctly all the time.
d) When line 34 is disconnected from the rest of the network, the downstream line cannot sustain as a smaller islanding network since no dedicated protection settings have been prepared for this condition.

The assumption in item (a) brings human fatality risk into acceptable region thus eliminating equipment damage possibility from the overall risk. Assumptions in (a) and (b) are likely to lead to an 'optimistic' risk result but as the purpose of the study is a comparative analysis between two protection approaches (i.e. adaptive and non-adaptive), making these simplifying assumptions for adaptive protection can be considered acceptable. This will become clearer when analysing the final results in section 7.8. Based on the assumption in (a) and (b), the risk assessment results of this case study cannot be used for any other intended use as they will not represent the actual risk of this adaptive scheme.

Data for the assessment are collected from literatures and results of the distribution network simulation. Fault simulation is carried out using Matlab software in order to calculate fault current at different position of the network during different network conditions. Detail of the network component models is described in appendix D.

Since in item (c) backup operation is asummed very reliable, hence any failures to operate of the adaptive protection will directly cause unecessary diconnnection of customers and generation(s).

7.4. Protection failure modes

There are three failure modes of the adaptive protection: failure to operate instantaneously (work in IDMT characteristics), failure to operate at all, and unwanted operation. Possible causes and consequences of each of the failure modes are summarised in Table 7.1. Some of the possible causes in the second column of Table II are not the root causes. For example, the protection setting updating failure can be caused by the network state detection failure or failure of the relay to change its settings.

Table 7.1. Failure modes, causes and consequences of the adaptive protection

Failure mode	Possible causes	Consequences
P34 failure to trip instantaneously for a fault in its protected zone	1. Protection settings updating failure for islanding state 2. A fault near the end of the line 3. A resistive fault	1. Operate in IDMT characteristic 2. WTG loss
P34 failure to operate for a fault in its protected zone	Protection component failure	Backup P23 operates, therefore Load 3 and WTG are lost
P43 failure to trip instantaneously for a fault in its protected zone	1. Protection settings updating failure for GTG 5 disconnected state 2. A fault near the beginning of the line 3. A resistive fault	No consequences as WTG's UV protection only depends on P34
P43 failure to operate for a fault in its protected zone	1. Protection settings updating failure for GTG5 disconnected state 2. Protection component failure	No consequences, assuming the remote backup is reliable
Unwanted operation of P34	1. Protection settings updating failure for grid connected state when a fault occurs downstream of line 34 2. Protection component unwanted operation (CB, relay)	Loss of loads and generators downstream line 34
Unwanted operation of P43	1. Human error causes setting updating failure for GTG5 reconnected state when a fault occurs upstream of line 34 or load current is higher than 90 A (instantaneous setting for GTG5 disconnected state) 2. Protection component unwanted operation (CB, relay)	Loss of loads and generators downstream of line 34

A fault on line 34 which initiates the trip of P43 will disconnect the rest of the downstream network from the system. Whether P43 succeeds to clear the fault on line 34 or its remote backup handles the clearing of the fault, the downstream network will remain disconnected. Moreover, GTG4 and GTG5 cannot create a smaller islanding network downstream line 34. Therefore, there is no consequence (and also no risk) of P43 failure to operate.

7.5. Modelling the risk of protection failure modes

Based on causes of the protection failure modes, model of the protection risk can be constructed. The models are constructed in Bayesian Network software: GeNIe [4].

7.5.1. Failure to operate of P34

P34 can fail to operate in two modes: failure to operate instantaneously and completely failure to operate. Therefore node ‘P34 failure to operate’ consists of four states i.e.:

- ‘Trip instantaneously’, the required states, is a condition when the protection trips immediately after occurrence of the fault hence avoids WTG disconnection.
- ‘Trip IDMT’ is a condition when the protection fails to trip instantaneously but able trip in longer time with the consequence of the WTG disconnection.
- ‘fail’ is a condition when the protection completely fails to operate hence causes the operation of backup protection (P23).
- ‘no faults’ is the condition when no faults occur in the protected line hence operation of the relay is not required.

The cause of the protection failure to operate when a fault occurs on the protected area is protection component failures or the adaptive setting failure. This causes are shown in Bayesian Network model in figure 7.3.

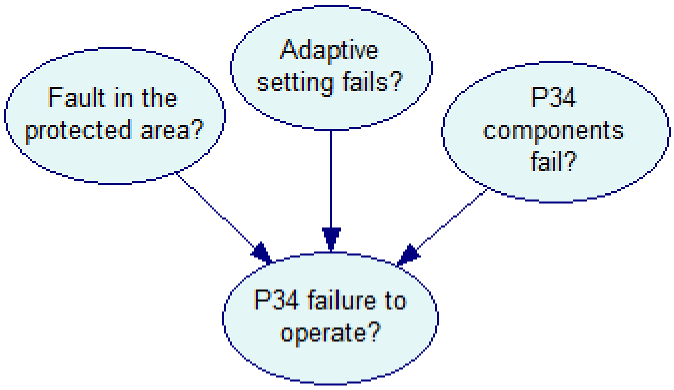

Figure 7.3. Causes of protection 34 failure to operate

The failure of the adaptive setting to apply a correct setting when the network is in islanding state is due to islanding detection failures. Similarly for the grid connected state, the adaptive setting failure is due to grid reconnected detection failure. In order to provide correct adaptive functionality, both hybrid and passive detections need to work correctly. Adding these detections system, the model becomes as shown in figure 7.4.

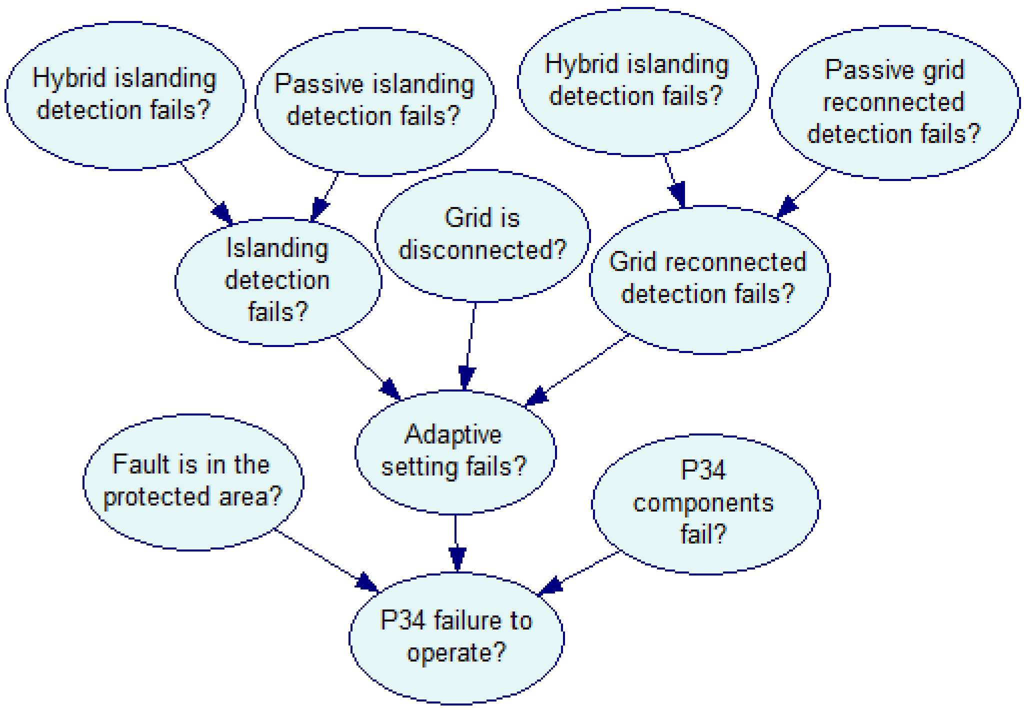

Figure 7.4. Model of protection 34 failure to operate

Since both of the passive detections are located in the same substation with P34 hence they share some equipment with P34. The shared equipment is VT and DC supply. The two hybrid detections is also share VT and DC supply. Adding the components of P34 and the detection schemes, the model is as shown in figure 7.5. If the islanding or grid reconnection occurs when the local demand in balance with the total DG's output then the hybrid detection need to increase or decrease the CHP generator output in order to detect the system state. Therefore if the CHP generation is not available during this condition, the islanding or grid reconnected detection will fail as shown in figure 7.5. The model in figure 7.5. also includes the effect of resistive fault as resistive faults will reduce the reach of the protection.

Figure 7.5. Model of protection 34 failure to operate

The consequence of failure to operate instantaneously of P34 is the disconnection of the WTG. Whereas the consequence of P34 failure to operate is the backup protection (P23) operation hence load 3 will be disconnected. The risk model is shown in figure 7.6 and will be used for the risk assessment model.

Figure 7.6. Risk model of P34 failure to operate

7.5.2. Unwanted operation of P34

From table 7.1, the sympathetic trips of P34 can be caused by settings updating failure for grid connected state when a fault occurs downstream of line 34. The unwanted operation can take place following a fault on line 45, line 56, GTG5's transformer or GTG5. Adding unwanted operation due to circuit breaker or relay spurious trip, the model for unwanted operation of protection 34 is as shown in figure 7.7.

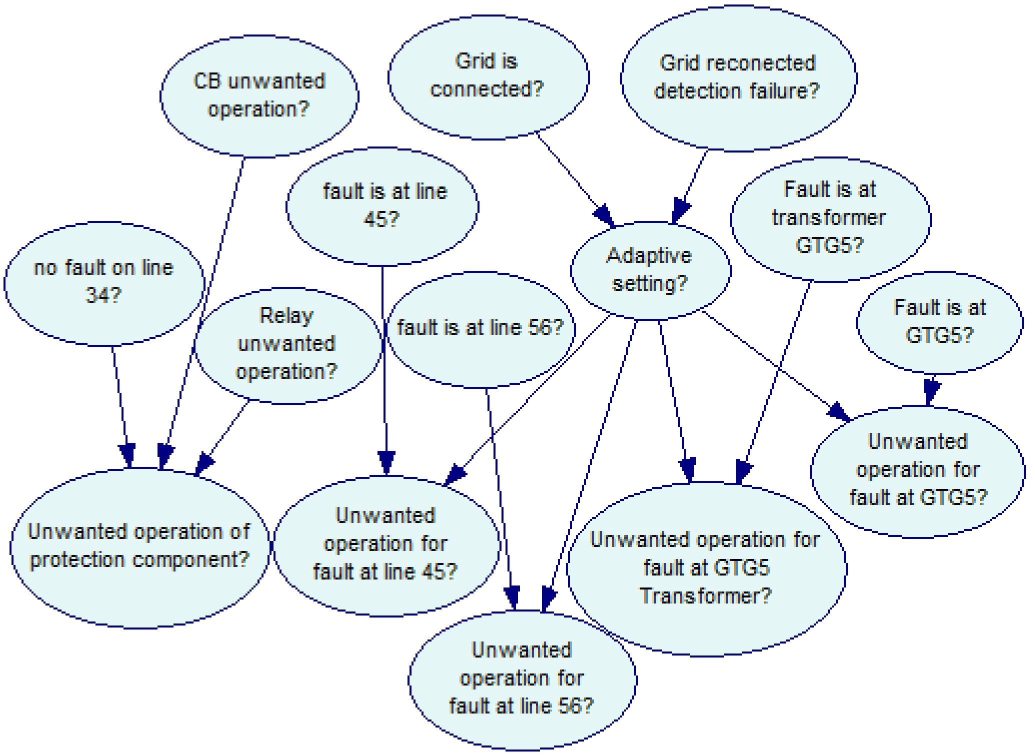

Figure 7.7. Model of unwanted operation of P34

Unwanted operations due to setting updating failure occur when the grid is in connected state while the protection setting is in islanding mode. This low setting causes operation of the relay for all downstream network faults.

The consequences of the unwanted operation depend on the initiating event as shown in table 7.2. The risk model of unwanted operation of P34 is as shown in figure 7.8.

Table 7.2. Consequences of P34 unwanted operation

Initiating event	Consequences
Relay or CB unwanted operation	Loss of Load 4, load 5, GTG4 and GTG5
Fault at line 45	Loss of load 4 and GTG4
Fault at line 56	loss of load 4, load 5 and GTG4
Fault at GTG5 transformer	loss of load 4, load 5 and GTG4
Fault at GTG5	loss of load 4, load 5 and GTG4

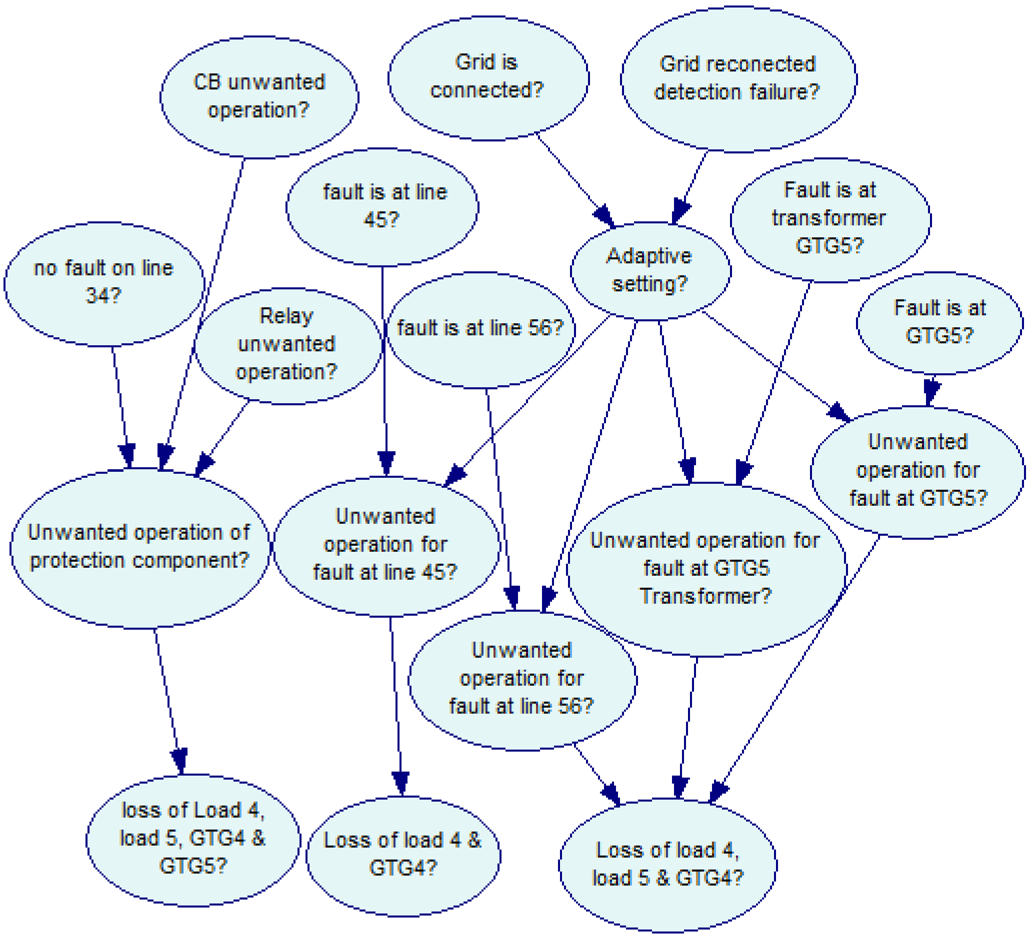

Figure 7.8. Risk model of unwanted operation of P34

7.5.3. Unwanted operation of P43

From table 7.1, the initiating events of unwanted operation of P43 are

- the relay or circuit breaker unwanted operation
- setting updating failures when GTG5 is reconnected.

The automatic setting change of P43 following reconnection of GTG5 is not included in adaptive functionality of the protection scheme design, therefore it is done manually by an operator. Consequently, the failures of the setting update will initiated by human error.

The failure to update the setting will cause sympathetic trip for any upper stream faults (on the lines, CHP transformers or CHP generators). Normal load current higher than 90A can also cause unwanted operation as the IDMT setting is 90A. The model of unwanted operation of P43 is shown in figure 7.9.

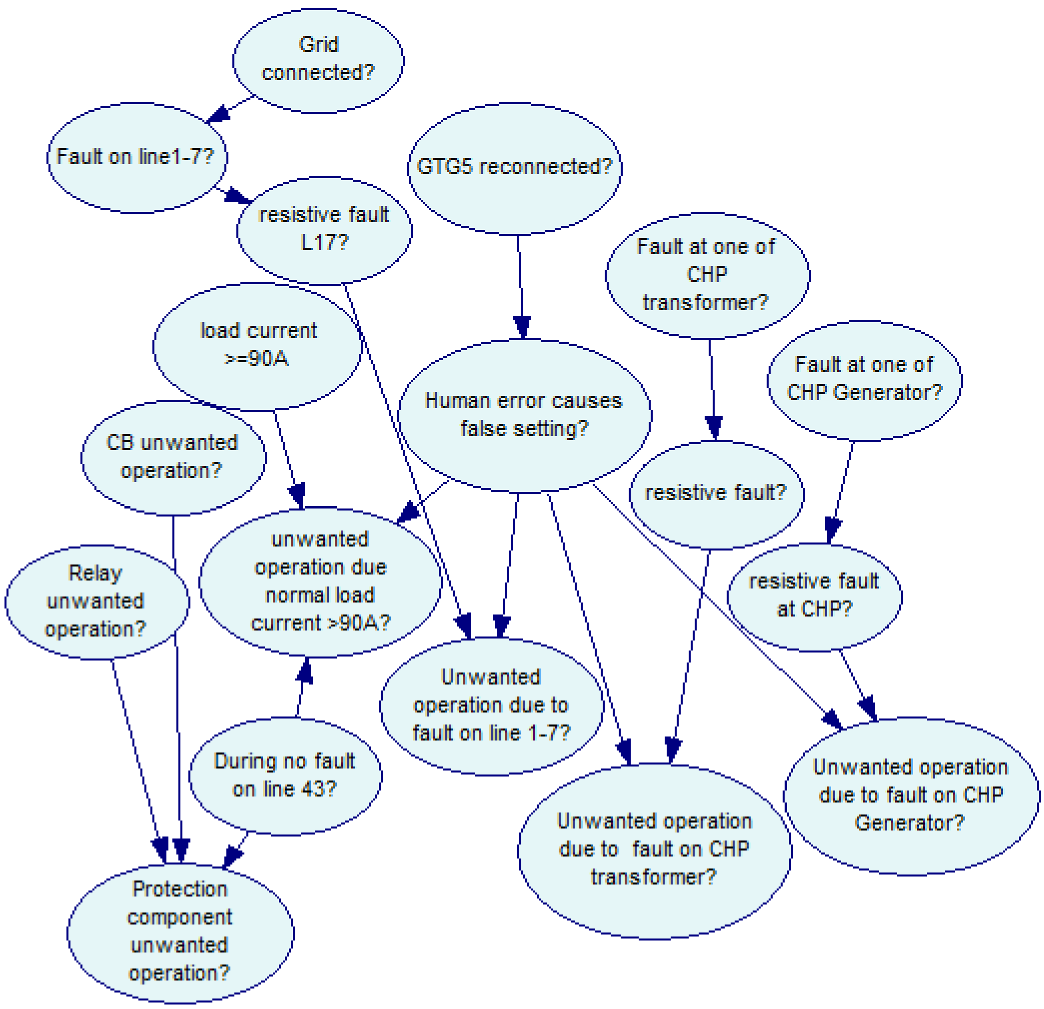

Figure 7.9. Model1 of unwanted operation of P43

Frequency of GTG5 reconnection is calculated based on the frequency of GTG5 disconnection because each disconnected event must be followed by a reconnection event. GTG5 disconnection can be triggered by the downstream protection operation to clear a fault (on line 46, GTG5 transformer, GTG5), planned and unplanned outage and any unwanted operation of protection on line 46 or at GTG5 plant. Adding these causes, the model becomes as shown in figure 7.10.

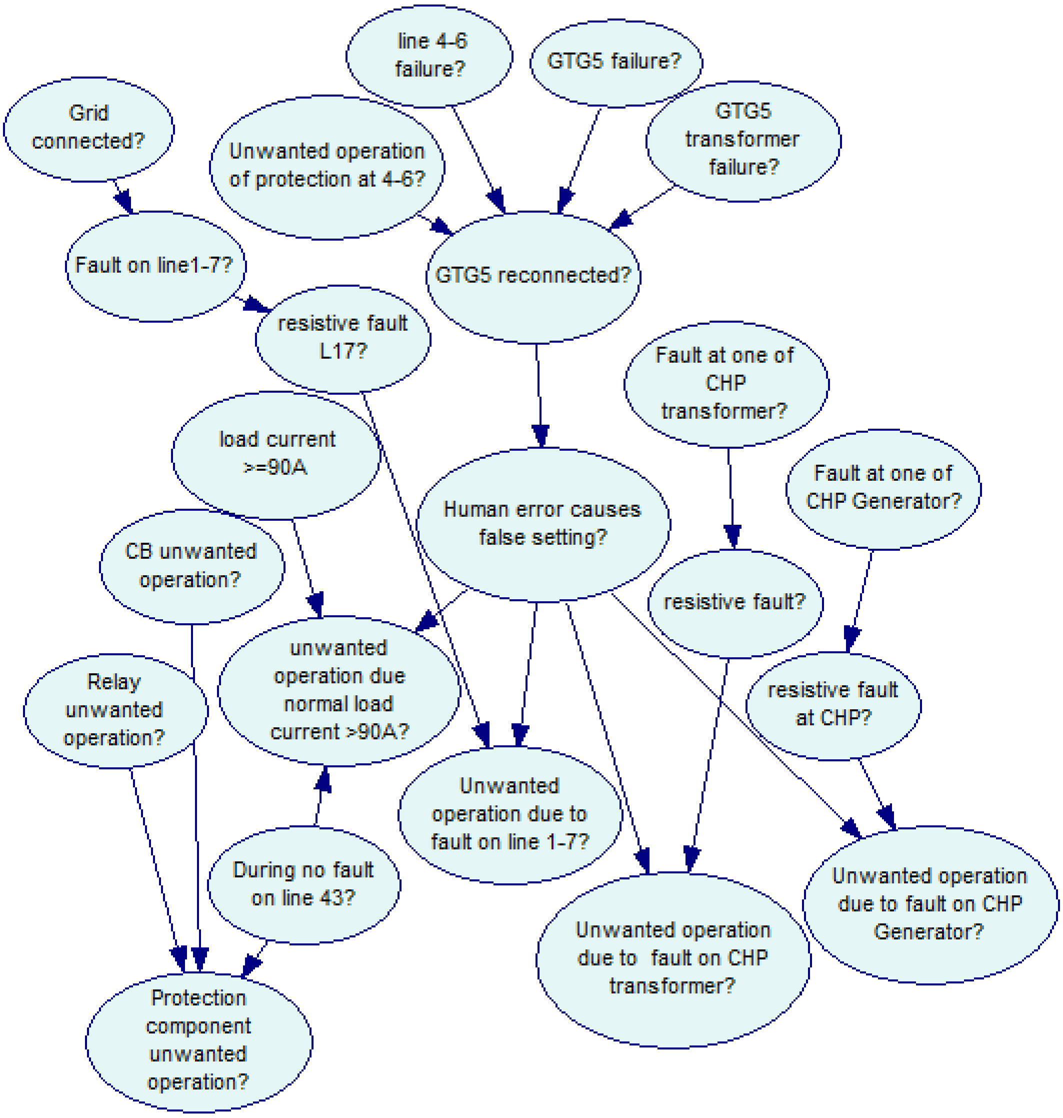

Figure 7.10. Model 2 for unwanted operation of P43

The consequences of the unwanted operation of P43 are as shown in table 7.3. There is no consequence for sympathetic trip for fault in line 1-3 as the fault already causes a power cut for the downstream network; hence it is not included in the model. Unwanted operation due to fault at line 17 has different impact which depends on the grid state. During grid connected state, it causes disconnection of Load 4, load 5, GTG4 and GTG5, but during grid disconnected state it does not have any impact as a fault on line 17 will cause power shortage and termination of the islanding operation.

Adding these consequences to the model in figure 7.10, the risk model of unwanted operation of P43 is as shown in figure 7.11.

Table 7.3. Consequences of unwanted operation of P43

Initiating event	Consequences
Relay or CB unwanted operation or line current>90A (the instantaneous setting for GTG5 disconnected state)	Loss of load 4, load 5, GTG4 and GTG5
Fault at line 13	No consequence
Fault at line 1-7	During grid connected, loss of load 4, load 5, GTG4 and GTG5
Fault at one of CHP Generator	Loss of load 4, load 5, GTG4 and GTG5
Fault at one of CHP transformer	Loss of load 4, load 5, GTG4 and GTG5

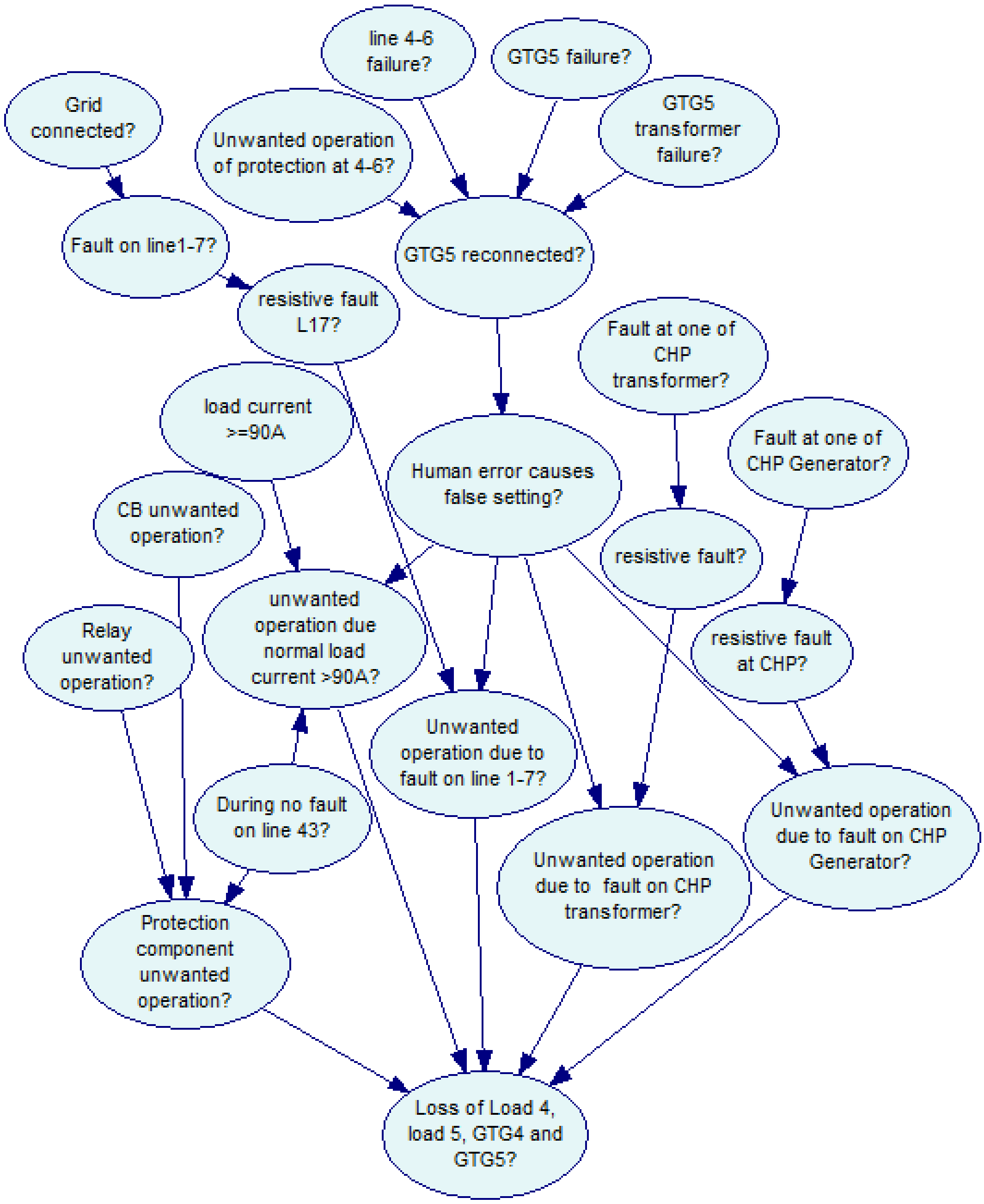

Figure 7.11. Risk model of unwanted operation of P43

7.6. Probability of the occurrence of failure modes

There are two metrics which will be used for the probability calculation i.e. unavailability and unreliability. The risks of failure to operate modes are calculated using the both probability metrics. The unreliability quantifies of failure frequency while the unavailability quantifies failure duration. Since the network is in a radial topology, duration of the protection failure consequence (loss of load, generation, etc.) is the same as the protection failure duration. Therefore the unavailability of the protection due to failure to operate modes determines the unavailability of the protection failure's consequences. However this is not the case for unwanted operation mode because the protection can be returned to service soon after its unwanted operation despite of the initiating event duration. The duration of the consequences of the protection unwanted operation can be found from statistical data. Therefore, in this case study, the probability of failure to operate modes will be calculated in unreliability and unavailability metrics whereas unwanted operation modes will be calculated in unreliability metric and assumed interruption/disconnection durations.

Unreliability parameter quantifies the probability of the occurrence of component/system first failure before the given mission time [4]. The chosen mission time of this case study is 24 hour duration (one day), instead of a year, in order to anticipate some initiating event which has MTTF of less than a year.

Fault simulation of distribution network in figure 7.1. is carried out at the beginning and the end of the lines during grid connected, islanding and GTG5 connected or disconnected using MATLAB software. The magnitudes of fault current (I_f) seen by relay 34 and 43 are then compared with the setting in order to know whether the relays will trip or not. The ratio of the protection trip is calculated as illustrated in figure 7.12 where the maximum and minimum fault currents seen by the relay for a given Z **Ω** fault impedance on line X-Y. The occurrences of the fault current are assumed in uniform distribution. The ratio of the protection trip for line faults on line 34 with Z ohm fault impedance is:

$$Trip\ ratio = \frac{C - B}{C - A} \tag{7.1}$$

Where

C= maximum fault current on line X-Y with Z ohm fault impedance

A= minimum fault current on line X-Y with Z ohm fault impedance

B= Setting of the relay

This ratio is calculated for different fault impedances and different grid short circuit powers and used as input for CPTs of the Bayesian network models.

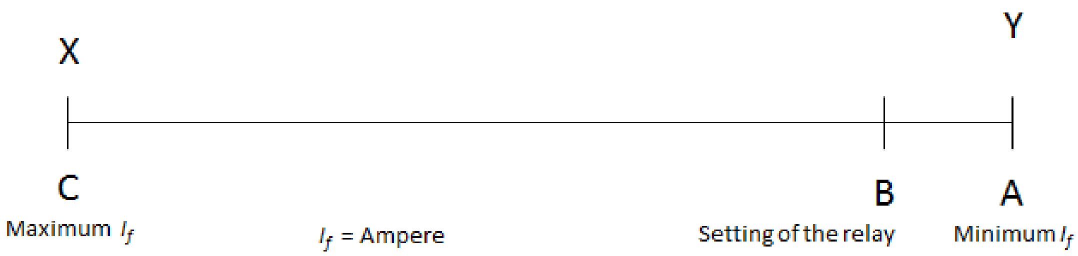

Figure 7.12. Fault currents of Z ohm fault impedance on line X-Y seen by the relay

Faults in underground distribution network according to [5] are mostly bolted, hence it is assumed that bolted fault is 90% of the total fault for the base case. Also based on the study by EPRI in [6], the maximum fault resistance in the underground distribution network which can be detected by protection is 2Ω. Therefore, the calculation is carried out with assumption that the resistances of the fault are varied in uniform distribution with the maximum 2Ω. The probability of the protection failure to operate instantaneously increases with the increasing resistance of the fault. In contrary, the probability of P43 unwanted operation is decrease with the increasing of resistance of the fault.

7.6.1. Probability of failure to operate of P34

The probability data of the P34 component failures are based on several literatures as shown in appendix D. Simulation of network faults is carried out in order to provide the CPT of node 'Protection 34 failure to operate?'. The simulation results also show that faults near the end of the line 34 cannot be detected by the both instantaneous setting (islanding or grid connected mode). It is because fault current is less than the settings and it becomes worse for resistive faults. The probabilities of undetected faults are calculated using equation (7.1). These probabilities are shown in table 7.4. which is the CPT of node 'P34 failure to operate?' in figure 7.6.

Table 7.4. CPT of node ‘P34 failure to operate?’

Bolted fault								
P34 component fail?	work				fail			
Adaptive setting fails?	undetected islanding	detected islanding	undetected grid reconnected	detected grid reconnected	undetected islanding	detected islanding	undetected grid reconnected	detected grid reconnected
instantaneous	0	0.9950217	1	0.869859147	0	0	0	0
IDMT	1	0.0049783	0	0.130140853	0	0	0	0
failure to operate	0	0	0	0	1	1	1	1
no fault	0	0	0	0	0	0	0	0

Resistive fault								
P34 component fail?	work				fail			
Adaptive setting fails?	undetected islanding	detected islanding	undetected grid reconnected	detected grid reconnected	undetected islanding	detected islanding	undetected grid reconnected	detected grid reconnected
instantaneous	0	0.144805	1	0.119132021	0	0	0	0
IDMT	1	0.855195	0	0.880867979	0	0	0	0
failure to operate	0	0	0	0	1	1	1	1
no fault	0	0	0	0	0	0	0	0

no fault								
P34 component fail?	work				fail			
Adaptive setting fails?	undetected islanding	detected islanding	undetected grid reconnected	detected grid reconnected	undetected islanding	detected islanding	undetected grid reconnected	detected grid reconnected
instantaneous	0	0	0	0	0	0	0	0
IDMT	0	0	0	0	0	0	0	0
failure to operate	0	0	0	0	0	0	0	0
no fault	1	1	1	1	1	1	1	1

The CPT in table 7.4. shows four states of node ‘P34 Failure to operate?, which are the possible states of the protection 34 i.e. ‘instantaneous’ (the successful operation), ‘IDMT’ (operating but resulting in some undesirable consequences), ‘failure to operate’ (totally fails to operate) and ‘no fault’ (the protection does not require to operate). The probability occurrence of each states of node ‘P34 failure to operate?’ is conditional upon the parent states. The parent nodes are ‘Adaptive setting fails?’, ‘P34 component fail?’ and ‘Resistive faults?’. For example, if node ‘Resistive faults?’ is in the ‘bolted fault’ state, node ‘P34 component fail?’ is in ‘work’ state and node ‘Adaptive setting fails?’ is in ‘undetected islanding’ state, therefore the probability of P34 operate in IDMT characteristic is 1 and other states are zero.

The calculated probability of failure to operate of protection 34 from the Bayesian Network software is shown in table 7.5.

Table 7.5. Probabilities of P34 failure to operate

Failure modes	Unreliability	Unavailability
Failure to operate instantaneously	1.30925154e-005	4.85294789e-006
Failure to operate	5.51356608e-009	2.1688522e-009

7.6.2. Probability of unwanted operation of P34

Fault simulation of grid connected state shows that any faults downstream of P34 have higher fault currents than instantaneous pickup setting of P34 in islanding mode. Therefore any of these faults will cause unwanted operation of P34 if the adaptive setting update for islanding condition fails. The unwanted operation probabilities of P34 are calculated from Bayesian network model in figure 7.8 as shown in table 7.6.

Table 7.6. Probabilities of unwanted operation of P34

Initiating event	Probability of unwanted operation of P34 (unreliability)
Protection component unwanted operation	1.74721573e-006
Faults at line 45	9.21983328e-009
Faults at line 56	9.21983328e-009
Faults at GTG5's transformer	1.91584005e-009
Faults at GTG5	1.25691465e-007

7.6.3. Probability of unwanted operation of P43

In the event of setting updating failure due to human error after GTG5 reconnected, the fault simulation shows that unwanted operation of P43 occurs for most of upper stream faults. This because the fault current when GTG5 is in connected state is higher than the protection instantaneous setting in islanding mode. Equation (7.1) is applied to calculate the probability of the protection trip. The probability of sympathetic trip for a fault in line 17 for example, is shown in table 7.7. which is the CPT of node ‘unwanted operation due to fault at line 1-7’ in figure 7.11.

Table 7.7. CPT of node ‘unwanted op for fault at line 1-7’

Human error causes false setting	no error			error		
Resistive fault in L17?	bolted	resistive	No fault	bolted	resistive	No fault
Unwanted operation	0	0	0	1	0.904347083	0
normal	1	1	1	0	0.095652917	1

Using Bayesian network model in figure 7.11, the probability of unwanted operation of protection 43 is as shown in table 7.8.

Table 7.8. Probabilities of unwanted operation of P43

Initiating event	Probability of unwanted operation of P43 (unreliability)
Protection component unwanted operation	1.74705918e-006
Normal current higher than 90 A	0.000163131442
Faults at line 17	7.16365047e-009
Faults at one of CHP’s transformer	4.76410947e-009
Faults at one of CHP generator	8.09637425e-010
Total unwanted operation	0.000164879597

7.7. Consequences of protection failure modes

From the models in section 7.5 can be seen that the consequences of the protection failure modes are unnecessary disconnection of load (customers) or/and generation. The cost of customer disconnection can be divided into 2 categories [7]:

- customer interruption cost which is related to frequency of disconnection
- cost of unsupplied energy which is related to duration of the disconnection

Similarly the cost of generation disconnection can also be divided into two categories:

- cost of shutdown and start-up which is related to frequency of disconnection
- profit loss due to unsupplied energy which is related to duration of the disconnection

For this case study, utilisation of more expensive generation from fast reserve is not applicable as the generation loss is small generators at the distribution level. The cost of customer and generation disconnection is shown in table 7.9.

Table 7.9. Interruption and unsupplied energy cost for demand and generation [8-11]

Disconnection	Interruption/shutdown-start-up cost (€/kW)	Unsupplied energy cost (€/kWh)
Customer	1.1	11
Onshore wind	0	0.003372
GTG	0.04085	0.00108

It is assumed the load factor of wind generation and biomass are 0.3 and 0.75 respectively and the customer demands are already in their averages, the cost of the disconnection is calculate as shown in table 7.10.

Table 7.10. Disconnection cost for demand and generation

Disconnection of	Rated power(kW)	Average power (kW)	Cost of interruption (€)	Cost of unsupplied energy (€/h)
WTG	2000	600	0	2.0232
Load 3	550	550	605	6050
load 4	850	850	935	9350
load 5	510	510	561	5610
GTG 4	3300	2475	101.10375	2.673
GTG 5	3300	2475	101.10375	2.673

7.8. Risk of the protection failure modes

Risk of the protection failure modes is calculated based on equations in (4.19), (4.20), (4.22) and (4.23). The risk results of the adaptive overcurrent protection are shown in table 7.11

Table 7.11. Risk of the adaptive overcurrent protection

Failure mode	P34 Risk (€/day)	P43 risk (€/day)
Failure to operate instantaneously	0.000235644	0
Failure to operate	0.000318358	0
Unwanted operation	0.0314764	2.7474800
Total Risk (€/day)	2.7795104	

For comparison, risks of applying conventional overcurrent protection for the same network without optimistic assumptions are calculated as shown in table 7.12. The conventional protection P34 and P43 use grid connected state setting and normal state settings respectively.

Table 7.12. Risk of the conventional overcurrent protection

Failure mode	P34 Risk (€/day)	P43 risk (€/day)
Failure to operate instantaneously	0.000235737	0
Failure to operate	0.000318561	0
Unwanted operation	0.0291148	0.0291148
Total Risk (€/day)	0.0587839	

From both results in table 7.11 and 7.12 can be seen that for the adaptive protection P34 the risk of non-instantaneous operation (i.e. delayed operation) and the risk of failure to operate are only slightly lower than for conventional protection scheme. Therefore, the advantage of the adaptive scheme to avoid disconnection of WTG during islanding condition using faster protection is only marginal. This is because the scheme cannot cover all possible faults experienced by the network (resistive faults for example), hence the reduction of risk is not significant.

Furthermore, the adaptive protection (P34 and P43) introduces a significant increase in risk unwanted operation compared to the conventional scheme. This is due to the possible failure to correctly detect grid reconnected state, as well as human failure to change the protection setting group for P43 after GTG5 reconnection. Although the risk assessment of the adaptive scheme is carried out under simplified optimistic assumptions where the state detection systems are assumed to be perfect, the risk result of the adaptive protection scheme is still higher than the conventional scheme (which was performed without those optimistic assumptions). Based on the total risk, it can be concluded that in this case the adaptive protection scheme does not provide better performance compared to the conventional scheme when applied to the same distribution system. It needs to be noted that this conclusion would still be valid even if the detection system was modelled in more realistically because the risk will be higher.

7.9. Sensitivity analysis

In order to find the most influential cause of the protection failure modes, the sensitivity analysis tool in the Bayesian Network is applied. The software will calculate the effect of small changes of probability of parent nodes to the output (failure mode probability). Based on this analysis, the most influence nodes from each failure modes are shown in table 7.13

Table 7.13. The most influenced nodes of protection failure modes

Failure mode	The most influenced nodes
Failure to operate of P34	The components failure of islanding detection, grid reconnect detection and adaptive protection
Unwanted operation of P34	CB and relay unwanted operation, failure of grid reconnect detection
Unwanted operation of P43	CB and relay unwanted operation, unwanted operation of protection in line 4-6, line 4-6 failure, GTG5 transformer failure, fault at CHP transformer and fault at CHP generator.

Table 7.13 shows that the most influenced nodes which generally can be divided into several categories: components of protection and detection scheme, fault in the network which cause GTG5 disconnection and a fault on CHP plants. However as the probability data of these nodes are based on statistical data, therefore they will not be included in sensitivity analysis.

7.9.1. Human error in changing P43 setting

The risk in table 7.11 demonstrates that the major risk of the adaptive protection come from unwanted operation of P43. The unwanted operation occurs if the operator fails to change the protection settings after GTG5 is reconnected to the network. The operator failing is a human error event. The probability for this event is taken from human error probability to open or close a circuit breaker i.e. six errors in 1000 manual switching [12].

Sensitivity analysis is carried out for smaller probability i.e. six errors in 10,000 , 100,000 and 1,000,000 switching operations. The results are shown in table 7.14. The results demonstrate that smaller human error probability cause smaller risk. However, even for extremely small human error probability i.e. 0.000006, the results still produce higher risk value of the adaptive protection compare to the conventional scheme.

Table 7.14. Protection risk for different of human error probability in changing the P43 setting

Human error probability	Risk of protection 43 unwanted operation (€/day)	Total risk (€/day)
0.006 (base case)	2.7474800	2.7795104
0.0006	0.3009499	0.3329794
0.00006	0.0562959	0.0883263
0.000006	0.0318306	0.0638610

7.9.2. Cost of failure mode consequences

The impact of the failure modes have been quantified using financial loss. However, data relating financial loss usually have a wide range and depend on the assumptions used in calculations. The data also vary according to time and place. If the consequences of failure modes are quantified using amounts of unsupplied energy due to load and generation disconnection, the results are as shown in table 7.15.

Table 7.15. Risk of the adaptive and conventional protection in term of unsupplied energy

Unsupplied energy due to:	Total risk from the adaptive protection (kWh/day)	Total risk from the conventional protection (kWh/day)
Load disconnection	0.227	0.005
Generation disconnection	0.895	0.087
Load & generation disconnection	1.122	0.092

The adaptive protection has significant unsupplied energy due to load or/and generation disconnection compare to the conventional protection. Therefore if amount of unsupplied energy is taken as the risk quantity, the adaptive protection is still has higher overall risk than conventional overcurrent protection.

Sensitivity analysis for other important nodes as stated in table 7.3 results in higher risk of the adaptive distance protection with the increasing failure probabilities of the node. While other nodes which are not listed in the table 7.3. do not have significant impact to the risk result.

7.10. Conclusion

The risk assessment has successfully revealed the risk of applying the adaptive overcurrent protection scheme for the case network. The adaptive overcurrent protection scheme can slightly reduce the risk of WTG disconnection during islanding, however it introduce significant higher risk of unwanted operation. From overall risk calculation, the adaptive scheme fails to provide lower risk level than conventional protection. Therefore this adaptive overcurrent protection scheme is not recommended to be applied in the distribution network.

7.11. References for Chapter 7

[1] P. Mahat, Z. Chen, B. Bak-Jensen, and C. L. Bak, "A Simple Adaptive Overcurrent Protection of Distribution Systems With Distributed Generation," *IEEE Transactions on Smart Grid,* vol. 2, pp. 428-437, Sept. 2011.

[2] P. Mahat, Z. Chen, and B. Bak-Jensen, "A hybrid islanding detection technique using average rate of voltage change and real power shift," *IEEE Transactions on Power Delivery,* vol. 24, pp. 764-771, 2009.

[3] P. Mahat, Z. Chen, and B. Bak-Jensen, "Control and Operational of Distributed Generation in Distributed Systems," *Electric Power Systems Research,* vol. 81, pp. 495-502, oct 2010 2011.

[4] H. Kumamoto and E. J. Henley, *Probabilistic Risk Assessment for Engineers and Scientists*, second ed. New York: IEEE Press, 1996.

[5] T. A. Short, *Electric Power Distribution Handbook*. Boca Raton: CRC Press, 2004.

[6] J. Burke. (2002, 18 Dec 2012). *Hard to find information about distribution system (28 August 2002 ed.)* [Reference Material]. Available: http://www05.abb.com/global/scot/scot235.nsf/veritydisplay/91ad3a29a50978bf85256c550053db0d/$file/hard.to.find.6th.pdf

[7] P. Verho, A. Mäkinen, K. Kivikko, S. Repo, P. Järventausta, T. Kaipia*, et al.*, "Visionary development of distribution networks," in *The 19th International Conference on Electricity Distribution (CIRED 2007)*, 2007.

[8] J. Valtari, P. Verho, A. Hakala-Ranta, and J. Saarinen, "Increasing cost-efficiency of substation automation systems by centralised protection functions," presented at the International conference and exhibition on electricity distribution, Prague, 2009.

[9] N. Kumar, P. Besuner, S. Lefton, D. Agan, and D. Hilleman, "Power Plant Cycling Costs," NREL, Colorado2012.

[10] IRENA, "Biomass for Power Generation," vol. 1: Power Sector, ed. Bonn: IRENA, 2012.

[11] D. Fouquet, "Prices for renewable energies in Europe: Report 2009," European Renewable Energies Federation, Brussels2009.

[12] R. R. Fullwood, *Probabilistic safety assessment in the chemical and nuclear industries*, 2 ed. Woburn: Butterworth-Heinemann, 2000.

Chapter 8. Conclusion, contribution and future work

The challenge of power system protection scheme selection is becoming more demanding due to the introduction of new generating and operational technologies in power system. Therefore, a more accurate selection process is needed. Risk assessment is proposed as an important complement to the existing protection selection process which can rank the protection candidates based on their overall expected performance. Moreover, risk assessment also offers a capability to establish optimum protection settings using protection failure modes as a basis. In order to facilitate application of risk assessment in power system protection selection and setting, a framework for power system protection risk assessment has been developed. It has been demonstrated that the proposed framework can be applied for evaluation of existing protection schemes after a change in the power system. The framework has been presented in this thesis along with its application through case studies. The key contributions of each chapter of the thesis have been summarised in the following section.

8.1. Review of chapter conclusions and contributions

Chapter 2.

Power system protection is an important safeguard to maintain power system operation. Protection failures will endanger the continuity of power system operation; therefore, the best protection must be chosen to minimize the risk. Existing protection selection practices are considered inadequate in ranking the protection candidates in many cases. The chapter also underlines the trends in future power systems which will be increasingly complex due to the introduction of new generating technologies. This exacerbates the existing protection selection practice. Due to the probabilistic nature of power system components and faults, a probabilistic method is considered most appropriate for a protection scheme selection method. This preliminary work has resulted in a successful conference paper contribution.

Chapter 3.

A review of risk assessment methodologies and approaches is reported on in this chapter. Risk assessment is a well-known method which has been successfully applied in many fields. However, its use in power system protection is not widely adopted. The need for a dedicated, clearly defined risk assessment framework for power system protection is therefore identified. The framework should be straightforward to apply, and the assessment results are convenient to be interpreted by the decision makers.

Chapter 4.

A dedicated risk assessment framework for power system protection is proposed and described. It consists of reason, intended use, scope of risk assessment, terminology and metrics, knowledge of the protection system and the protected system, system scenario, data and assumptions, the risk assessment steps and decision making. The thesis suggests employing Bayesian Network as a probability calculation technique. However, the framework can be implemented using other probability calculation technique and applied for any risk assessment tasks. This work has laid a foundation to a paper which will be submitted to a journal.

Chapter 5.

Chapter 5 presents a case study which demonstrates application of the proposed risk assessment approach for evaluation of existing protection after introducing certain changes in the primary system. In the case study, installation of a quadrature booster transformer has negative effect on the performance of the existing distance protection. Risk assessment is carried out to evaluate the protection performance in terms of risk in order to make a decision whether the existing protection can be maintained, or needs to be replaced or modified. The applied assumptions in this study have simplified the scenarios and model for the assessment. The results show that the risk resulting from the quadrature booster operation to the protection is relatively small. Therefore, the existing protection can be maintained. The result corresponds with current practice in National Grid where existing distance protection schemes are maintained to work without any modification. Part of the work in this case study has contributed to a conference paper.

Chapter 6.

A second case study which demonstrates investigation of the optimal protection settings using the proposed risk assessment framework is presented. The risk assessment is shown to be successful in finding the optimum setting for GB's ROCOF protection. The optimum setting which considers year 2020 power system scenario, provides a trade-off between the risk of failure to operate and unwanted operation. The work for this case study has contributed to a conference paper.

Chapter 7.

The final case study, presented in chapter 7, has been summited as a journal paper. The case study demonstrates application of the proposed risk assessment framework as a tool for the selection of power system protection scheme. The case study addresses a key question relating to whether the proposed adaptive overcurrent protection scheme is a proper choice to deal with islanded operation of the distribution network with distributed generators. After applying the proposed risk assessment method, it is apparent that the adaptive protection candidate fails to demonstrate improved performance over the existing scheme in terms of risk. This work has contributed to a journal paper (under review)

8.2. Conclusion

The thesis has proposed, described and demonstrated an effective, risk based method for power system protection assessment and selection. The method overcomes the limitations of existing protection scheme selection practices. A dedicated risk assessment framework for power system protection has been proposed to help protection engineer in conducting the assessment, reporting on the risk assessment process, and presenting the results. Three case studies have been included to illustrate the practical implementtions of the risk assessment. It has been shown that the risk assessment can be applied successfully in:

- evaluation of the existing protection schemes following a change in the primary system configuration,
- finding optimum setting of a protection scheme, and
- selection of the best protection scheme from alternative candidates.

8.3. Future work

The research presented in this thesis can be further developed in the following ways:

- Numerical protection is gradually replacing older generation relays. Future protection schemes are likely to become “smart” with the capability to adapt to changing primary system condition. This adaptive capability needs to be supported by reliable software. Such software, due to its complexity, can become an initiating event for the protection failure modes. Therefore, the author believes that software failure should be included in the future risk assessment of power system protection.
- In the case study of adaptive overcurrent protection (refer to chapter 7) human error is one of the initiating events for the protection failure mode. In order to simplify the assessment, the case study only uses data for human error to open or close a circuit breaker. However, to increase the accuracy of future protection risk assessment, a dedicated human error risk assessment is suggested. Software and human error risk assessment are considered very complex. However, in order to better reflect realty in the future, they might be needed. Protection scheme which provides good risk results but has an extremely complex algorithm or setup will be more prone to software and/or human error related failure. Therefore, software and human error assessment can be a measure of protection simplicity.
- The research has been carried out without considering protection unavailability due to maintenance. Since the maintenance duration and frequency may vary for each protection candidate, it will result in different

availability and risk of the protection candidates. Therefore, unavailability of the protection due to maintenance should be included in the future work.

- An important consideration in protection scheme selection is the cost and the benefit of utilising of the protection candidates or called risk-benefit analysis. Risk-benefit analysis should be carried out after completing the risk assessment as it can provide more detailed guidance in the decision process.
- The risk assessment framework can be implemented within protection risk assessment software to realise a degree of automation in conducting the risk assessment with reduced requirements for manual data entry. Therefore, the methodology can be applied more conveniently including for engineers who are not fully-familiar with risk assessment theory and practice.

Appendix A. Data for case study distance protection with QB

Data of the primary system and its protection for case study in chapter 5 are taken from [1]. The substation data are shown in table A.1, distance protection related data are shown in table A.2 and table A.3 shows the transmission line data.

Table A.1. Substation data [1]

Substation	Voltage (KV)	Fault level (KA)	X/R	Z_s (ohm)	$<Z_s$ (°)
RATS	400	38.52	12	5.9953	85.24
WBUR	400	39.66	12	5.823	85.24
HIGM	400	30.8	12	7.4981	85.24
GREN	400	31.64	12	7.229	85.24
WILE	400	38.22	12	6.0424	85.24
STAY	400	28	12	8.2479	85.24
COTT	400	46.22	12	4.9965	85.24

Table A.2. Distance protection data [1]

Protection parameter	Configuration
RCA	84.67°
CT ratio	1000/1
CVT ratio	40kV/110V
Tripping	3 pole

Table A.3. Transmission line data [1]

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

A.1. Reference for Appendix A

[1] I. F. Abdulhadi, "Facilitating the Validation of Adaptive Power System Protection through Formal Scheme Modelling and Performance Verification," PhD, Electronic aand Electrical Engineering, Strathclyde, Glasgow, 2013.

Appendix B. Predicted Great Britain Power System Condition for year 2020.

The predicted condition is based on National Grid gone green scenario for year 2020 which is collected from publication at National Grid website http://www2.nationalgrid.com/UK/industry-information/. These data are used for case study 'finding ROCOF protection optimum setting' in chapter 6.

B.1. GB power system model

Power system is modelled as in figure 6.15 and utilised generic model of DIgSILENT Power Factory components i.e. wind generator, synchronous generator, two winding transformer, general load, synchronous motor, and shunt capacitor. The simulation results i.e. ROCOF of the system, are validated to the National Grid simulation result in publication [1].

B.2. Average loading factor and capacity of synchronous machine based DG

Capacity of synchronous machine based DG in 2020 is predicted in National Grid's Ten year statement [2]. Using generic loading factor of generation technology in [3], the average loading factor can be calculated as:

$$LF = \frac{\sum_i^n LF_i \times C_i}{\sum_i^n C_i}$$

Where: LF_i = loading factor DG with technology i

C_i = Capacity of DG with technology i

The average loading factor of DG types and the predicted capacity in 2020 is as shown in table B.1 The average loading factor of the synchronous DG in 2020 will be:

$$LF = \frac{(0.353 \times 0.62) + (0.60 \times 4.9) + (0.625 \times 2.69)}{8.21} = 0.589538368$$

Table B.1. Average loading factor and capacity of synchronous machine technology DG

DG type	Loading factor	Predicted capacity (GW)
Hydro	0.353	0.62
CHP	0.6	4.9
Biomass	0.625	2.69
Total	-	8.21
Average for one DG	0.589538368	0.0117

Average of one DG capacity in 2020 is assumed the same as current average. Current average one DG capacity is calculated from [4] where total capacity is 4322.9MW and consist of 371 DG hence the average one DG capacity is 4322.9/371 = 11.7MW. For year 2020 there are around 4GW DG with ROCOF protection with average capacity 11.7 hence number of DG with ROCOF protection:

$$N_{ROCOF} = \frac{total\ DG\ capacity}{average\ DG\ capacity} = \frac{4000}{11.7} = 341.88 \cong 342$$

B.3. DG Profit

Profit of DG is calculated as :

(consumer price of electricity + ROC) – (cost of generating the electricity from DG + distribution network charges).

The consumer price of electricity from [5] for domestic consumer and from [6] for non-domestic consumer is shown in table B.2. Around 40% of electricity in GB is consumed by domestic consumer and 60% for non-domestic consumer [7]. Taking these percentages for calculating average price of electricity, the average electricity price is £120.4/MWh.

Table B.2. GB Electricity prices 2013 excluding climate change Levy tax

Consumer type	Pence/kwh
Domestic	15.2
nondomestic:	
Very Small	13.12
Small	11.51
Small/Medium	10.19
Medium	9.23
Large	8.65
Very Large	8.48
Extra Large	8.52
Average	9.79
nondomestic average	9.935830443
Total average £/MWh	120.4149827

ROC (Renewable Obligation Certificate) is a certificate issued to operator of renewable generation for renewable energy they generate. ROC can be sold to other supplier who does not have sufficient ROC to fulfil the obligation. The price of ROC changes according the market and it becomes additional income for renewable generation operator. The average ROC price in December 2013 was £43/ROC [8]. Depend on type of generation each MW power output has different value of ROC as shown in table B.3.

Table B.3. ROC for different DG and the average capacity in 2020 [9],[2]

Generation technology	ROC (£/MWh)	ROC x Capacity (£)
Hydro	1	43
CHP	1.5	64.5
Biomass	0.5	21.5
average DG ROC price (£/MWh)		48.78411452

The cost of electricity generation from a power plant is based on levelised value of electricity generation. Levelised value is calculated as a ratio of present value of total capital and operating cost of a generic plant to total output of the plant over its operation life. Levelised costs of the generation technology are shown in table C.4. The average levelised cost is based on predicted capacity of each technology as in table B.4.

Table B.4. Levelised cost [10]

Generation	levelised cost (£/MWh)
Biomass	120.67
CHP	103
Hydro	116.33
Average	109.8

Distribution Network Operator (DNO) charges the generator for using their network to deliver the power to consumer. The cost consists of unit rate, fixed charge and reactive power charge as shown in table C.5. for DNO Electricity North West Limited.

Table C.5. Distribution network charges components

Unit rate (p/KWh)	fixed charge p/day	reactive charge p/KVArh
4.546	6.36	0.125

Using this data for output 11.7MW/h with pf 0.9 and loading factor 0.59, the network charge is £46.0052/MWh. Based on these prices, cost and charge, the profit of DG is:

120.4149827 + 48.78411452 - 109.8 - 46.0052 = £ 13.40/MWh.

B.4. Generator shutdown-start-up (cycling) cost

There are three type of synchronous technology-DGs in GB system i.e. CHP, biomass and hydro. CHP and biomass shutdown-start-up cost is assumed based on the shutdown-start-up cost of combine cycle of gas generator which is $35/MW-capacity for hot-start [11]. This is equivalent with £21.41/MW-capacity using 2011 exchange rate. For hydro generation, the cycling cost is £3/MW-capacity [12] or equivalent with £1.92/MW-capacity. Average of these two cycling cost based on each DG type capacity, is £19.94/MW-capacity and it becomes the average cycling cost of the synchronous technology DGs.

B.5. Fast Reserve Generation Utilisation Cost

National Grid uses fast reserve generation to provide rapid and reliable active power delivery following sudden and sometimes unpredicted change of generation or demand. The price of utilisation fast reserved is based on monthly tender. The average utilisation cost for 2013 is £143.28/MWh [13]. The average price of electricity in GB is £120.41/MWh [5], hence the additional cost of fast reserved utilisation is £22.87/MWh.

B.6. Duration of maintenance on the HV islanding network

In order to predict the probability of occurrence of electrical worker in a distribution network, frequency and duration of maintenance work in each distribution network component is calculated. The job titles of the maintenance work and their frequencies are collected from [14]. Duration of each works is assumed. The total duration for the whole HV network of a distribution system is as shown in table B.6.

Table B.6. Frequency and duration of maintenance activity in a distribution network [14]

No	Asset	Maintenance task	frequency	duration each (minutes)	quantity	Total duration/ year (minutes)
1	Distribution line	Inspection of poles, cross-arms, insulators, conductors and misc. fittings	5 years' scheduled works	20	400	1600
		Inspection of tubular steel poles for earthing integrity	5 years' scheduled works	20	400	1600
		Structural assessment of urban wooden angle poles and wooden termination poles.	10 years' scheduled works	10	100	100
		Excavate and inspect lattice steel tower grillages	15 years' scheduled works	20	100	133.333333
		Vegetation management	3-5-yearly patrols	5	600	1000
2	Substation transformer, tap changer and earthing	Visual inspection oil leakage, mechanical deterioration, earthing Integrity, breather maintenance, fans/pumps operational checks	3 monthly	60	5	1200
		Tap-changer contact and mechanism maintenance	3 yearly service	60	5	100
3	Circuit-breakers, ABS, Reclosers	Visual inspection for oil leakage, mechanical deterioration	3-monthly	60	10	2400
		Operational tests on CBs not operated in last 12 months. Condition-test switchgear including thermal, PD and acoustic emission scan	12-monthly checks	60	10	600
		Clean bushings, IR test, mechanical checks	3-yearly service	60	8	160
4	Ground mounted transformer and voltage regulator	Inspect ground-mounted transformers for environment issues, such as oil leaks, graffiti and damage caused by other parties	6 monthly	20	5	200
		Inspect ground-mounted transformer tanks and general fittings for corrosion, damage, etc.	1 year	20	5	100
		Thermal scans of voltage regulator HV terminals and isolator switches	2.5 years	20	5	40

		Carry out transformer and voltage regulators earth bond and electrode resistance tests	5 years	15	5	15
		Carry out voltage regulator windings condition tests	15 years	15	5	5
		Specific maintenance as result of condition monitoring	Condition based	120	1	60
5	Pole mounted distribution transformer	Inspect pole-mounted transformer tank and general fittings for corrosion and inspect earthing connection	5 years	30	1	6
6	HV Capacitor	Inspect all HV capacitor for damaged bushes, corroded tanks, oil leaks, automatic controller operation	12 months	20	3	60
		Thermal scans of all capacitor HV connectors	2.5 years	20	3	24
		Carry out condition-assessment measurements	10 years	30	3	9
7	Network air-break switches built-up areas	Contacts & jumpers thermal scanning at	5-yearly intervals	10	2	4
		Operation and major maintenance of contacts, pantographs, mechanisms, etc.	at 5-yearly intervals	120	2	48
8	Network air-break switches - rural areas	Visual Inspections of contacts, pantographs, etc	at 5-yearly intervals	10	3	6
		Operation and major maintenance	at 10-yearly intervals	120	3	36
9	Line Recloser and sectionaliser	RTU battery checks at	12-monthly intervals	30	3	90
		Thermal scans of jumpers	at 2½-yearly intervals	20	3	24
		Interrupter condition tests of vacuum & gas interrupters	at 10-yearly intervals	20	3	6
		Major contacts & tank maintenance of oil reclosers	at 5-yearly intervals	60	3	36
		External inspections of vacuum & gas interrupter units	at 5-yearly intervals	20	3	12
		Major maintenance of vacuum & gas recloser mechanisms	at 10-yearly intervals	180	3	54

10	Substation indoor switchgear	Visual inspections in zone substation	at 3-monthly	20	5	400
		Zone substation circuit breaker trip tests at	12-monthly intervals	30	5	150
		Zone substation switchboard acoustic & thermal condition scans at	12-monthly intervals	20	5	100
		Zone substations switchboard partial discharge locator tests at	6-yearly intervals	30	5	25
		Zone and distribution substations circuit breaker tripping operation tests	at 12-monthly intervals	30	5	150
		Major contacts & tank maintenance of zone substation oil circuit breakers	at 3-yearly intervals	60	5	100
		Zone substations vacuum & gas interrupter contacts wear & gas pressure checks	3-yearly intervals	20	5	33.3333333
		Zone substations vacuum & gas circuit breaker interrupter withstand tests	at 6-yearly intervals	30	5	25
		Major contacts & tank maintenance of distribution substation oil circuit breakers	at 5-yearly intervals	30	5	30
		Distribution substation vacuum & gas interrupter contacts wear & gas pressure checks	at 5-yearly intervals	20	5	20
		Distribution substation vacuum & gas circuit breaker interrupter withstand tests	at 10-yearly intervals	30	5	15
11	Ground mounted distribution switch gear	Partial discharge & acoustic emission scans of oil, gas & vacuum switchgear at 12-monthly	at 12-monthly	30	5	150
		Thermal scans of all switchgear	at 5-yearly	20	5	20
		Oil swithgear sample tested	10 yearly	20	5	10
		Safety inspections of all ground-mounted switchgear	at 6-yearly intervals	30	5	25

		Inspections for weeds, condensation, graffiti, electrical discharge, corrosion, etc. of all ground-mounted switchgear	at 12-months intervals	30	5	150
		Service switchgear actuators and batteries	at 2½-yearly	30	5	60
		Shutdown and service contacts, clean and service cast resin switchgear in all other regions	at 5-yearly intervals	30	5	30
		Operate, clean and lubricate oil, gas and vacuum switchgear mechanisms	at 5-yearly intervals	60	5	60
12	Zone substation SCADA RTU batteries and charging system	Inspection of battery hazard signs, cases, plates, vent plugs, terminals, connections, electrolyte levels (where applicable) and general condition assessment	3 monthly	30	5	600
		Charger alarms giving correct status and general condition assessment	3 monthly	30	5	30
		Battery-type, capacity and performance correct for site load, discharge test,check charging current/voltage	12-monthly scheduled	30	5	150
		Chargers set correctly, within limits, in good condition and type suitable for site load	12-monthly scheduled	20	5	100
13	Distribution substation SCADA RTU batteries and charging systems	Inspection of battery hazard signs, cases, plates, vent plugs, terminals, connections, electrolyte levels (where applicable) and general condition assessment	3-monthly	30	5	600
		Charger alarms giving correct status and general condition assessment	3 monthly	20	5	400
		Battery type, capacity and performance correct for site load, discharge test, check charging current/voltage	12-monthly scheduled work	20	5	100
		Chargers set correctly, within limits, in good condition and type suitable for site load	12-monthly scheduled works	20	5	100
14	Load Control plants	Check and inspect mechanical condition of plant Operational checks for successful transmission, signal levels and abnormal vibrations	3-monthly	30	3	360
		Perform diagnostic tests	Annually	30	3	90
15	Protection and control equipment	Inspection for physical damage	3-monthly checks	30	10	1200
		Functional tests, relay pick-up tests	3-yearly service	30	10	100

16	Back-up generation equipment	Run-up and run-down testing	Monthly	30	5	1800
		Minor servicing	Quarterly	60	5	1200
		Major servicing	Annually	240	5	1200
TOTAL maintenance (minutes/year)						19311.6667

B.7. References for Appendix B

[1] National-Grid, "Frequency Changes during Large Disturbances and their Impact on the Total System," National Grid, London2013

[2] National_Grid, "Electricity Ten Year Statement," National Grid, London2012.

[3] NETS_SQSS, "Transmission Entry Working Group," National Grid2012.

[4] DCRP_Secretary, "Progress of Distributed Generators in Changing Frequency Protection Settings to Comply with ER G59/2," DCRP2012.

[5] I. MacLeay. (2014, March 2014). Domestic energy bills in 2013: The impact of variable consumption. *Energy trends statistical March*

[6] J. Marvin, "prices of fuels purchased by non domestic consumers in the United Kingdom excluding/including CCL," DECC, Ed., ed: Department of Energy & Climate Change, 2014.

[7] M. Gregory, S. Khan, and S. Stadnyk, "Sub-national Electricity Consumption Statistics," Department-of-Energy&Climate_Change, Ed., ed. London, 2013.

[8] NFPA. (2013, February). *Track Record ROC price*. Available: http://www.e-roc.co.uk/trackrecord.htm

[9] Department-of-Energy&Climate_Change. (Pebruary). *Renewable Oblogation Certificate (ROC) Banding*. Available: http://chp.decc.gov.uk/cms/roc-banding/

[10] Department-of-Energy&Climate-Change, "Electricity Generation Cost," London2012.

[11] N. Kumar, P. Besuner, S. Lefton, D. Agan, and D. Hilleman, "Power Plant Cycling Costs," NREL, Colorado2012.

[12] O. Nilsson and D. Sjelvgren, "Hydro unit start-up costs and their impact on the short term scheduling strategies of Swedish power producers," *Power Systems, IEEE Transactions on,* vol. 12, pp. 38-44, 1997.

[13] National_Grid, "Fast Reserve, Market Information for Tenders for March 2013 - March 2014," National grid, London2013-2014.

[14] Powerco, "Our Assets. Asset Management Plant 2013," Powerco, New Plymouth2013.

Appendix C. Data of distribution network test system, UKGDS EHV1

The UKGDS EHV1 network is used to analyse the risk from unwanted operation of ROCOF protection scheme due to nearby faults for case study in chapter 6. The EHV1 model is a 33kV rural network fed from a 132kV supply point. The network has long lines, including a sub-sea cable between buses 318 and 304. This network was created by Centre for Sustainable Electricity and Distributed Generation (http://www.sedg.ac.uk/) [1]. Single line diagram is shown in figure B.1. and its numerical data are in table C1 to C6

Table C.1. Generator data [1]

Bus no	P (MW)	Pmax (MW)	Pmin (MW)	Q (MVAr)	Qmax (MVAr)	Qmin (MVAr)	R1 (pu) gen base	X1(pu) gen base	R0(pu) gen base	X0(pu) gen base
100	30	60	-60	10	60	-60	0	0.05	0	0.05
336	0	15	-15	0	15	-15	0	0.5	0	0.5

Table C.2 . Load data [1]

Bus	P(MW)	Q(MVAr)	Bus	P(MW)	Q(MVAr)
1101	1.9	0.39	1110	0.06	0.01
1102	1.5	0.3	1111	0.55	0.11
1103	0.28	0.06	1112	0.04	0.01
1104	0.32	0.06	1113	0.77	0.15
1105	3.31	0.67	1114	2.7	0.55
1106	1.93	0.39	1115	2.85	0.58
1107	18.4	3.74	1116	0.8	0.16
1108	1.9	0.39	1117	0.21	0.04
1109	0.06	0.01	1118	0.58	0.12

Table C.3 .Transformer data [1]

From	To	R_1 (pu)	X_1(pu)	R_0 (pu)	X_0 (pu)	R-earth (pu)	Rating MVA	winding connection	phase shift angle
100	302	0	0.25	0	0.25	50	33	DY	-30
100	302	0	0.25	0	0.25	50	33	DY	-30
301	1101	0.381	2.978	0	1.9858	0	2.75	DY	-30
303	1102	0.517	4.019	0	2.8895	0	2.2	DY	-30
304	321	0.073	0.104	0	0	0	16.5	DD	0
306	1103	1.580	12.120	0	10.100	0	0.55	DY	-30
308	1104	1.580	12.120	0	10.100	0	0.55	DY	-30
309	1105	0.151	1.614	0	1.6144	20.026	5.5	DY	-30
310	1106	0.092	1.055	0	1.0553	20.026	11	DY	-30
312	1107	0.034	0.892	0	0.8925	19.776	27.5	DY	-30
313	1107	0.034	0.893	0	0.8925	19.776	27.5	DY	-30
315	1108	0.384	2.997	0	1.9986	0	2.75	DY	-30
317	1109	2.714	20.781	0	17.317	0	0.55	DY	-30
319	1110	2.714	20.781	0	17.317	0	0.55	DY	-30
321	1111	0.797	6.175	0	5.1461	0	1.1	DY	-30
322	1114	0.384	2.997	0	1.9986	0	2.75	DY	-30
322	1114	0.384	2.997	0	1.9986	0	2.75	DY	-30
324	1112	2.714	20.781	0	17.317	0	0.55	DY	-30
325	1113	0.743	5.760	0	4.7997	0	1.1	DY	-30
326	1115	0.094	1.087	0	1.0869	39.704	11	DY	-30
328	1116	0.743	5.760	0	4.7997	0	1.1	DY	-30
330	1117	0.580	4.492	0	3.5703	0	1.65	DY	-30
334	1118	1.010	7.7911	0	6.4926	0	1.1	DY	-30

A synchronous technology DG with capacity 30 MW is inserted in bus 318 to represent a DG with ROCOF protection. The system utilised DIgSILENT Power Factory standard model for the system components.

Table C.4 . Line data in 100MVA base [1]

From	To	R1 (pu)	X1(pu)	B1(pu)	R0(pu)	X0(pu)	B0(pu)	Rated (MVA)	Lenght (km)
302	303	0	0.001	0	0.001	0.001	0	44	0.08
302	327	0.213	0.284	0	0.64	0.852	0	22	8.69
302	331	0.091	0.121	0	0.273	0.364	0	22	3.71
302	340	0.227	0.302	0	0.681	0.907	0	22	9.24
302	341	0.104	0.199	0	0.311	0.596	0	27.5	6.3
303	305	0.128	0.094	0	0.379	0.28	0	16.5	2.75
303	339	0.1	0.225	0	0.299	0.674	0	27.5	6.1
305	306	0	0.001	0	0.001	0.001	0	33	1.03
305	307	0.056	0.041	0	0.168	0.124	0	16.5	1.14
307	308	0.002	0.001	0	0.006	0.004	0	16.5	0.04
307	309	0.507	0.374	0	1.521	1.123	0	16.5	10.34
310	311	0.216	0.287	0	0.648	0.862	0	22	8.79
311	312	0.03	0.026	0.002	0.047	0.049	0.002	22	2.14
311	313	0.031	0.032	0.001	0.064	0.075	0.001	22	1.97
311	314	0.517	0.376	0	1.55	1.126	0	16.5	10.53
311	338	0.079	0.106	0	0.238	0.317	0	22	3.23
314	315	0.009	0.007	0	0.027	0.02	0	16.5	0.18
314	316	0.166	0.121	0	0.499	0.363	0	16.5	3.39
316	301	0.228	0.227	0	0.685	0.682	0	16.5	6.76
316	317	0	0.001	0	0.001	0.001	0	33	0.92
318	304	0.336	0.27	0.006	0.572	0.584	0.006	16.5	12.32
318	319	0	0.001	0	0.001	0.001	0	33	0.93
320	321	0	0.001	0	0.001	0.001	0	33	0.91
320	322	0.538	0.733	0	1.613	2.198	0	16.5	22.28
322	323	1.126	0.873	0.001	3.33	2.477	0.001	16.5	23.33
322	326	0.944	0.657	0	2.833	1.971	0	16.5	19.05
323	324	0.045	0.02	0	0.134	0.059	0	11	0.46
323	342	0.238	0.173	0	0.715	0.519	0	16.5	4.86
327	328	0.053	0.023	0	0.158	0.069	0	11	0.54
327	329	0.094	0.11	0.001	0.247	0.31	0.001	16.5	3.69
329	330	0.039	0.039	0	0.117	0.117	0	16.5	1.16
329	337	0.083	0.083	0	0.249	0.248	0	16.5	2.46
331	332	0.113	0.1	0.002	0.234	0.261	0.002	16.5	4.22
332	333	0.153	0.203	0	0.457	0.609	0	22	6.21
334	333	0.149	0.108	0	0.446	0.325	0	16.5	3.04
335	334	0.4	0.291	0	1.2	0.872	0	16.5	8.16
335	336	0.401	0.292	0	1.204	0.875	0	16.5	8.19
337	335	0.088	0.088	0	0.264	0.263	0	16.5	2.61
338	318	0.026	0.016	0.001	0.033	0.025	0.001	16.5	0.9
339	310	0.098	0.221	0	0.294	0.663	0	27.5	5.95
340	311	0.216	0.287	0	0.648	0.862	0	22	8.79
341	311	0.208	0.398	0	0.624	1.195	0	27.5	12.63
342	325	0.226	0.164	0	0.677	0.492	0	16.5	4.6

Table C.5 . Number of faults on UKGDS components [1,2]

Distribution Line					
No	from	to	Failure rate (f/km/y)	Length (km)	no of fault/year
1	302	303	0.034	0.08	0.00272
2	302	327	0.034	8.69	0.29546
3	302	334	0.034	17.18	0.58412
4	302	340	0.034	9.24	0.31416
5	302	341	0.034	6.3	0.2142
6	303	305	0.034	2.75	0.0935
7	303	310	0.034	12.05	0.4097
8	305	306	0.034	1.03	0.03502
9	305	307	0.034	1.14	0.03876
10	307	308	0.034	0.04	0.00136
11	307	309	0.034	10.34	0.35156
12	310	311	0.034	8.79	0.29886
13	311	312	0.034	2.14	0.07276
14	311	313	0.034	1.97	0.06698
15	311	314	0.034	10.53	0.35802
16	311	318	0.034	4.13	0.14042
17	314	315	0.034	0.18	0.00612
18	314	316	0.034	3.39	0.11526
19	316	301	0.034	6.76	0.22984
20	316	317	0.034	0.92	0.03128
21	318	304	0.034	12.32	0.41888
22	318	319	0.034	0.93	0.03162
23	320	321	0.034	0.91	0.03094
24	320	322	0.034	22.28	0.75752
25	322	323	0.034	23.33	0.79322
26	322	326	0.034	19.05	0.6477
27	323	324	0.034	0.46	0.01564
28	323	325	0.034	9.46	0.32164
29	327	328	0.034	0.54	0.01836
30	327	329	0.034	3.69	0.12546
31	329	330	0.034	1.16	0.03944
32	329	335	0.034	5.07	0.17238
33	335	334	0.034	8.16	0.27744
34	335	336	0.034	8.19	0.27846
35	340	311	0.034	8.79	0.29886
36	341	311	0.034	12.63	0.42942
Transformer					
No	from	to	Failure rate (f/y)	number	no of fault/year
37	100	302	0.0392	2	0.0784
38	301	1101	0.01	1	0.01
39	303	1102	0.01	1	0.01
40	304	321	0.01	1	0.01

41	306	1103	0.01	1	0.01
42	308	1104	0.01	1	0.01
43	309	1105	0.01	1	0.01
44	310	1106	0.01	1	0.01
45	312	1107	0.01	1	0.01
46	313	1107	0.01	1	0.01
47	315	1108	0.01	1	0.01
48	317	1109	0.01	1	0.01
49	319	1110	0.01	1	0.01
50	321	1111	0.01	1	0.01
51	322	1114	0.01	1	0.01
52	322	1114	0.01	1	0.01
53	324	1112	0.01	1	0.01
54	325	1113	0.01	1	0.01
55	326	1115	0.01	1	0.01
56	328	1116	0.01	1	0.01
57	330	1117	0.01	1	0.01
58	334	1118	0.01	1	0.01
Bus					
No	Bus no		Failure rate (f/y)	number	no of fault/year
59	301		0.08	1	0.08
60	302		0.08	1	0.08
61	303		0.08	1	0.08
62	304		0.08	1	0.08
63	305		0.08	1	0.08
64	306		0.08	1	0.08
65	307		0.08	1	0.08
66	308		0.08	1	0.08
67	309		0.08	1	0.08
68	310		0.08	1	0.08
69	311		0.08	1	0.08
70	312		0.08	1	0.08
71	313		0.08	1	0.08
72	314		0.08	1	0.08
73	315		0.08	1	0.08
74	316		0.08	1	0.08
75	317		0.08	1	0.08
76	318		0.08	1	0.08
77	319		0.08	1	0.08
78	320		0.08	1	0.08
79	321		0.08	1	0.08
80	322		0.08	1	0.08
81	323		0.08	1	0.08
82	324		0.08	1	0.08
83	325		0.08	1	0.08
84	326		0.08	1	0.08
85	327		0.08	1	0.08
86	328		0.08	1	0.08

87	329		0.08	1	0.08
88	330		0.08	1	0.08
89	331		0.08	1	0.08
90	332		0.08	1	0.08
91	333		0.08	1	0.08
92	334		0.08	1	0.08
93	335		0.08	1	0.08
94	336		0.08	1	0.08
95	337		0.08	1	0.08
96	338		0.08	1	0.08
97	339		0.08	1	0.08
98	340		0.08	1	0.08
99	341		0.08	1	0.08
100	342		0.08	1	0.08

Total faults = 11.96548 faults/year.

According to [3], faults on the distribution network the consist of three phase fault 0.048770575, phase to phase fault 0.095162582 and single phase fault 0.121904569, hence taking the same type of fault percentage to the total faults, number of fault in the network according the type is as shown in table B.6.

Table C.6 . Annual number of fault on the UKGDS network according to fault types

Type of fault	Number of fault/year
Three phase	2.19518634
Phase to phase	4.28331218
Single Phase to ground	5.48698148

C.1. References for Appendix C

[1] C. Foote. UKGDS EHV1 [Online]. Available: https://www.dropbox.com/s/e5pu0gkaxzyq17h/UKGDS_WebSiteContent.zip

[2] I. S. Ilie, I. Hernando-Gil and S. Z. Djokic, "Reliability equivalents of LV and MV distribution networks," in *Energy Conference and Exhibition (ENERGYCON), 2012 IEEE International*, 2012, pp. 343-348.

[3] A. A. Chowdhury and D. O. Koval, Eds., *Power Distribution System Reliability, Practical Methods and applications* (IEEE press series on power engineering. New Jersey: John Willey & Sons, 2009, p.^pp. Pages.

Appendix D. Data for adaptive overcurrent protection case study

D.1. Primary system data

Data of primary system for case study adaptive overcurrent protection are given in the table D1 to D3 i.e. distribution lines, generator and load, wind and gas turbine generator. The voltage level of the distribution network is 20 kV.

Table D.1. Data of distribution lines [1]

From bus	To bus	Resistance (Ω)	Reactance (Ω)
1	7	0.1256	0.1404
1	2	0.1344	0.0632
2	3	0.1912	0.0897
3	4	0.4874	0.2284
4	5	0.1346	0.0906
5	6	0.1346	0.0906

Table D.2. Generator and load data [1, 2]

Load/Generator	P (kW)
Load 3	550
Load 4	850
Load 5	510
WTG	2000
GTG1	3300
GTG2	3300
GTG3	3300
GTG4	3300
GTG5	3300

Maximum grid short circuit power 249 MVA

Minimum grid short circuit power 224 MVA

Table D.3. Data of wind turbine generator and gas turbine generator [1, 2]

Parameters	Wind turbine generator	Gas turbine generator
Rated power	2000 k VA	3300 kVA
Step–up transformer	20/0.4 kV	20/6.3 kV
Stator resistance	0.0108 pu	0.0504
Stator reactance	0.0121 pu	0.1
Magnetic reactance	3.362 pu	
Synchronous reactance d-axis		1.5 pu
Synchronous reactance q-axis		0.75 pu
Transient reactance d-axis		0.256
Subtransient reactance d-axis		0.168
Subtransient reactance q-axis		0.184
Transient time constant d-axis		0.53 s
Sub.trans. time constant d-axis		0.03
Sub.trans. time constant q-axis		0.03
Rotor resistance	0.004 pu	
Rotor reactance	0.05 pu	
Crowbar resistance	0.5 pu	
Crowbar reactance	0.1 pu	
Inertia time contant	0.38 s	0.54 s
Rotor inertia	61×10^5 kgm^2	
Nominal turbine speed	18 rpm	
Rotor radius	50m	
Max. Current for crowbar insertion	5 kA	

D.2. Network modelling and simulation

Turbine gas generators are modelled as synchronous generators which having nominal voltage sources behind subtransient impedances. Wind turbine generator is modelled as an asynchronous generator which having a crowbar in series with rotor winding for the fault current greater than 5 kA. Grid is modelled as a synchronous generator having short circuit impedance. The fault current of simulation results are validated to data presented in literature [1].

D.3. Data of protection component failures

Data of component failures of the case study adaptive overcurrent protection is shown table D.4.

Table D.4. Protection component failure data

No	Component	failure rate	MTTF (hour)	MTTR (hour)	unavailability	Unreliability (a day)	Source
1	Grid disconnection	0.0375 failure/year	233600	140	5.9896E-04	0.0001	[3, 4]
2	Circuit breaker 20 kV	MTTF=75 years	657000	12	1.8265E-05	3.6529E-05	[5]
3	Circuit breaker unwanted operation	0.000287375 failure/year	47479674.8	12	2.5274E-07	7.87328E-07	[6]
4	CT (10-30kV)	MTTF=500 year	4380000	7	1.5982E-06	5.47944E-06	[5]
5	VT (10-30kV)	MTTF=500 year	4380000	7	1.5982E-06	5.47944E-06	[5]
6	numerical relay	0.0124 fault/year	706451.6	48	6.794E-05	3.3972E-05	[7, 8]
7	Relay spurious trip	0.0003504 spurious trip/year	25000000	1	4E-08	9.6E-07	[9]
8	DC Power System (battery)	0.0006 failure/year	14600000	10.33	7.075E-07	1.64383E-06	[10]
9	wiring	0.0012 failure/year	7300000	11.2	1.53E-06	3.28767E-06	[10]
10	20 KV underground distribution line	0.028 fault/km/year	312857.1	8.9	2.8447E-05	7.67094E-05	[11, 12]
11	GTG not in operation	10.1 failure/year	867.2	14.8	0.01678	0.027295825	[10]
12	DG transformer failure	0.0032 failure/year	2737500	60	2.1917E-05	8.76708E-06	[10]

13	Microcontroller for islanding detection	0.00876 failure/year	1000000	3 assume	3.0E-06	2.39997E-05	[13]
14	Human error for change the relay setting group				6.00E-03		[14]
15	Electric fault on Generator of GTG system	0.21 failure/year	41714.3	4.1	9.828E-05	0.000575177	[10]

D.4. References for appendix D

[1] P. Mahat, Z. Chen, B. Bak-Jensen, and C. L. Bak, "A Simple Adaptive Overcurrent Protection of Distribution Systems With Distributed Generation," *IEEE Transactions on Smart Grid*, vol. 2, pp. 428-437, Sept. 2011.

[2] P. Mahat, Z. Chen, and B. Bak-Jensen, "A hybrid islanding detection technique using average rate of voltage change and real power shift," *IEEE Transactions on Power Delivery*, vol. 24, pp. 764-771, 2009.

[3] A. Dysko, I. Abdulhadi, X. Li, and C. Booth, "Assessment of Risk Resulting from the Adjustment of ROCOF Based Loss of Mains Protection Settings, Phase I " University of Strathclyde, Glasgow2013.

[4] I. S. Ilie, I. Hernando-Gil, and S. Z. Djokic, "Reliability equivalents of LV and MV distribution networks," in *Energy Conference and Exhibition (ENERGYCON), 2012 IEEE International*, 2012, pp. 343-348.

[5] M. H. J. Bollen, "Literature Research for Reliability Data of Components in Electric Distribution Networks," Eindhoven University of Technology, EindhovenAugust 1993 1993.

[6] C. R. Heising, E. Colombo, A. L. J. Janssen, J. E. Maaskola, and E. Dialynas, "Final Report on High-Voltage Circuit Breaker Reliability Data for Use In Substation and System Studies," presented at the Cigre Session, Paris, 1994.

[7] E. O. Schweitzer, B. Flemming, T. J. Lee, and P. M. Anderson, "Reliability Analysis of Transmission Protection Using Fault Tree Methods," presented at the Western Protective Relay Conference, 1997.

[8] V. Gurevich, "Reliability of Microprocessor-Based Protective Devices Revisited," *Journal of Electrical Engineering*, vol. 60, pp. 1-6, 2009.

[9] IEEE, "IEEE Std 500-1984 Circuit Breakers, Interrupters, Relays, Switches, and Fuses -- Preface," in *IEEE Std 500-1984*, ed. New York: IEEE, 1983, pp. 97-214-54.

[10] "IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems (Gold Book)," *IEEE Std 493-1997 [IEEE Gold Book]*, pp. 1-464, 1998.

[11] Y. HE, "Reliability of distribution network components," presented at the International conference on electricity distribution, Prague, 2009.

[12] A. A. Chowdhury and D. O. Koval, Eds., *Power Distribution System Reliability, Practical Methods and applications* (IEEE press series on power engineering. New Jersey: John Willey & Sons, 2009, p.^pp. Pages.

[13] R. Bell, "Introduction and revision of IEC 61508," in *Advances in Systems Safety*, ed: Springer, 2011, pp. 273-291.

[14] R. R. Fullwood, *Probabilistic safety assessment in the chemical and nuclear industries*, 2 ed. Woburn: Butterworth-Heinemann, 2000.