



REPORT N° 70038087-03

RESPOND –
ADAPTIVE PROTECTION
SAFETY JUSTIFICATION
ISSUE 2

CONFIDENTIAL

JUNE 2018

RESPOND - ADAPTIVE PROTECTION SAFETY JUSTIFICATION

Electricity North West Ltd

**Issue 2
Confidential**

Project no: 70038087
Date: June 2018








WSP
Manchester Technology Centre
Oxford Rd, M1 7ED
Manchester

Tel: +44 (0) 161 200 5000

www.wsp.com



QUALITY MANAGEMENT

ISSUE/REVISION	FIRST ISSUE	ISSUE 2	REVISION 2	REVISION 3
Remarks	Issue 1	Issue 2		
Date	April 2018	June 2018		
Prepared by	G Bennett, M Irwing	M Irwing		
Signature				
Signature				
Checked by	G Williamson	Stephen Elliott		
Signature				
Authorised by	S Elliott	Stephen Elliott		
Signature				
Project number	70038087	70038087		
Report number	70038087-03	70038087-03		

PRODUCTION TEAM

CLIENT

Innovation Engineer Kieran Bailey

Innovation Delivery Manager Paul Turner

WSP

Project Manager Gillian Williamson

Technical Specialist Peter Watson

Safety Specialist Gary Bennett

Mike Irwing

Project Engineer Gerasimos Doris

GLOSSARY

1oo1	One out of One
1oo2	One out of Two
ALARP	As Low As Reasonably Practicable
AP	Adaptive Protection
BM	Balancing Mechanism
CB	Circuit Breaker
CT	Current Transformer
DC	Direct Current
DNO	Distribution Network Operator
ENA	Energy Networks Association
ENW	Electricity North West
ETA	Event Tree Analysis
FCL	Fault Current Limiting
FLAT	Fault Level Assessment Tool
FLMT	Fault Level Mitigation Technique
HAZOP	Hazard and Operability
HV	High Voltage
HSE	Health and Safety Executive
H&S	Health and Safety
IPCT	Interposing Current Transformer
LCNF	Low Carbon Network Fund
LV	Low Voltage
NAFIRS	National Fault and Interruption Reporting Scheme
NMS	Network Management System
Ofgem	Office of Gas and Electricity Markets
QRA	Quantitative Risk Assessment
SDRC	Successful Delivery Reward Criteria
SFAIRP	So Far As Is Reasonably Practicable
SIL	Safety Integrity Level
SIPS	System Integrity Protection Scheme
UKPN	UK Power Networks

TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
1 INTRODUCTION.....	3
1.1 INTRODUCTION	3
1.2 THE RESPOND PROJECT	3
1.3 REQUIREMENT FOR SAFETY JUSTIFICATION	3
1.4 SAFETY JUSTIFICATION PROJECT	5
1.5 REPORT STRUCTURE.....	5
2 SAFETY ASSESSMENT APPROACH.....	6
2.1 REVIEW OF LEGISLATION AND REGULATORY REQUIREMENTS	6
2.2 ESTABLISHING RISK CRITERIA	6
2.3 SAFETY ASSESSMENT METHOD	7
2.4 SYSTEM DEFINITION.....	8
2.5 HAZARD IDENTIFICATION.....	8
2.6 INITIAL RISK ASSESSMENT.....	8
2.7 RISK ASSESSMENT PRINCIPLE	8
2.8 CODES OF PRACTICE.....	8
2.9 QUANTIFIED RISK ASSESSMENT	8
2.10 SAFETY REQUIREMENTS.....	8
2.11 PROJECT SAFETY ORGANISATION	9
2.12 MANAGEMENT, REVIEW AND APPROVAL	10
3 ADAPTIVE PROTECTION.....	11
3.1 INTRODUCTION	11
3.2 DEFINITION.....	11
3.2.1 INSTALLATION.....	11
3.2.2 OPERATION	13
3.2.3 ENHANCED PROTECTION WITH REDUNDANCY	14

3.2.4	NETWORK CONDITIONS	15
3.2.5	MAINTENANCE	15
3.3	EXISTING USAGE	15
3.4	REFERENCE SYSTEM.....	16
4	TOLERABILITY OF RISK FRAMEWORK.....	18
5	LEGISLATIVE REVIEW	22
5.1	LEGISLATIVE FRAMEWORK.....	22
5.2	DISCUSSION OF REQUIREMENTS	22
6	HAZARD IDENTIFICATION AND QUANTIFIED RISK ASSESSMENT	24
6.1	IDENTIFIED HAZARDS	24
6.2	QRA METHODOLOGY	24
6.3	INPUT DATA	24
6.3.1	FREQUENCY OF INITIATING EVENTS	24
6.3.2	PROBABILITY OF AP FAILURE	25
6.3.3	PROBABILITY OF WORKER FATALITY	26
6.3.4	PROBABILITY OF PUBLIC FATALITY.....	26
6.4	QRA RESULTS	27
6.5	DISCUSSION OF RESULTS.....	28
6.6	SENSITIVITY ANALYSIS.....	28
6.7	IMPLICATIONS OF 1001 AND 1002 SOLUTIONS.....	29
6.8	SAFETY REQUIREMENTS.....	29
6.9	NEXT STEPS.....	30
7	CONCLUSIONS.....	31
7.1	SUMMARY	31
7.2	FURTHER DEVELOPMENT TO SUPPORT FUTURE IMPLEMENTATION	32

BIBLIOGRAPHY	33
APPENDIX A HAZARD LIST	I
APPENDIX B EVENT TREES	III
APPENDIX C SAFETY REQUIREMENTS	VIII
APPENDIX D KEY REQUIREMENTS OF HEALTH & SAFETY APPLICABLE LEGISLATION	X

TABLES

TABLE 3-1	ADAPTIVE PROTECTION PARAMETERS.....	12
TABLE 4-1	RISK MATRIX (PER HAZARD) - WORKERS.....	19
TABLE 4-2	RISK MATRIX (PER HAZARD) – PUBLIC	20
TABLE 4-3	CONSEQUENCE CLASSIFICATIONS.....	20
TABLE 4-4	RISK MATRIX CALIBRATION	20
TABLE 6-1	FREQUENCY OF INITIATING EVENTS	25
TABLE 6-2	AP FAILURE INPUT DATA.....	25
TABLE 6-3	QRA RESULTS.....	28

FIGURES

FIGURE 1-1	RESPOND SAFETY JUSTIFICATION PROJECT TASKS.....	5
FIGURE 2-1	RESPOND PROJECT SAFETY ASSESSMENT PROCESS	7
FIGURE 2-2	SAFETY JUSTIFICATION DELIVERY AND RESPONSIBILITY ORGANISATION.....	9
FIGURE 3-1	STANDARD ADAPTIVE PROTECTION – RADIAL FEEDERS.....	12
FIGURE 3-2	STANDARD ADAPTIVE PROTECTION – CLOSED RING.....	13
FIGURE 3-3	DENTON WEST – SINGLE LINE DIAGRAM	17
FIGURE 3-4	ADAPTIVE PROTECTION – DENTON WEST CONFIGURATION	17
FIGURE 4-1	HSE FRAMEWORK FOR THE TOLERABILITY OF RISK.....	18
FIGURE 4-2	SPECIFIC BOUNDARY VALUES FOR RESPOND PROJECT	19
FIGURE 4-3	ENA RISK ASSESSMENT TOOL - EXTRACT FROM ENA SHE STANDARD 07 MDSR.....	21
FIGURE 6-1	RESPOND AP RISKS 1001 (NO REDUNDANCY, SIL 2 SYSTEM)	27
FIGURE 6-2	RESPOND AP RISKS 1002 (WITH REDUNDANCY, SIL 3 SYSTEM)	27

EXECUTIVE SUMMARY

ENW's Respond project is trialling new methods of mitigating fault level issues as alternatives to expensive replacement of equipment. The Respond project is a Low Carbon Network Fund (LCNF) Tier 2 project, which is funded by the Low Carbon Innovation Fund.

One of these methods is Adaptive Protection (AP) which uses protection relay functionality at 11kV substations where potential fault levels exceed equipment ratings. AP works by sensing a fault current and automatically reconfiguring the network to limit potential fault current before the circuit breaker is opened to clear the fault as normal. This prevents equipment ratings being exceeded and provides safe operation of equipment.

This safety justification is required to satisfy the LCNF project's Successful Delivery Review Criteria. It has been produced by WSP, independently from ENW, with input from and peer review by other DNO(s) and presented to HSE to demonstrate that a robust approach has been taken.

A safety assessment has been undertaken to develop this safety justification for the implementation of the defined AP scheme within the ENW network. Key outcomes of the safety assessment are summarised below.

The safety assessment has categorised substation sites as low, medium or high risk in order to assign a range of measured safety requirements. In simple terms low risk sites are rural and not densely populated, medium risk sites are typical urban locations and high risk sites are in continuously busy, densely populated areas. The analysis has shown that, based on arguably conservative assumptions, it would be acceptable from a safety viewpoint to fit substations with an AP system provided that they are not high risk sites and that an AP in one out of one (1oo1) configuration is used for low risk sites and one out of two (1oo2) configuration for high risk sites. The 1oo1 configuration would be required to meet the SIL2 requirements of BS EN 61508 and the 1oo2 configuration would need to meet SIL3.

The safety assessment process has determined three hazard scenarios presenting the most significant risk. These include the possibility of exploding feeder cables, fire in substations, and structural damage to substations. These hazards could potentially result in injuries and fatality to workers and members of the public.

Safety requirements have been established (further to those already in place for the existing network and operations) which would ensure control of the risk associated with each of these scenarios to a 'Tolerable' level. The safety requirements include:

- a) Application conditions that must be satisfied before applying AP to a site, i.e. pre-requisites
- b) Safety function and performance measures necessary for the AP system, including safety integrity level
- c) Implementation, operating and maintenance measures necessary to control safety risk of the AP scheme in use, including compliance with safety management systems, standards, procedures and codes of practice.

The study has also reviewed the requirements laid down by the health and safety applicable legislation. This identified 'absolute' requirements of the Electricity At Work (EAW) Regulations, specifically Regulations 5, 11 and 12 which, unlike other legislation requirements, are not satisfied by 'reasonably practicable' risk control measures and safety arguments. The EAW Regulations, Regulation 29, sets out the means for a legal defence in the event these 'absolute' regulations are breached.

This point has been discussed with HSE and the HSE's view was that provided a risk assessment had been performed which justified that the risk presented by the AP scheme was 'Broadly Acceptable' then this would support an ENW claim that it had taken sufficient steps to comply with the Regulations.

The safety assessment study has therefore considered steps that could be taken by ENW to demonstrate that risks associated with the defined AP scheme are 'Broadly Acceptable' for all scenarios.

Introducing a 1002 configuration for the AP relay moves the residual risk for all but one scenario into the 'Broadly Acceptable' region. Further risk reduction measures would be required to protect the public at high risk sites, e.g. at a shopping centre.

By ensuring that substation structures and cable routes are able to contain the effects of explosion and fire at high risk sites, they would then become medium or low risk sites and the risk associated with the scenario would then become 'Broadly Acceptable'.

The study considered the robustness of the input data and assumptions and determined that some current data and assumptions could be over-pessimistic. Where a justification could be made to refine these then that may remove the need for the additional measures for substation structures and cable ducts at high risk sites and may also allow other sites to be fitted with a 1001 AP configuration.

It should be noted that amongst the requirements for application of AP it is necessary that the busbar itself and the feeder circuit breakers are able to withstand the fault currents that will occur up until the point at which AP is guaranteed to operate (approximately 400ms). Ability to meet this condition has not yet been demonstrated by the AP development team but is a clear pre-requisite for application of AP.

1 INTRODUCTION

1.1 INTRODUCTION

Electricity North West (ENW) commissioned WSP to assess the safety of the three Fault Level Mitigation (FLM) techniques being trialled by their Respond project and to assess compliance of the techniques with the relevant UK legislation.

WSP has prepared this Safety Justification independently as part of an unbiased and robust approach to assess the safety of the Respond FLM techniques.

1.2 THE RESPOND PROJECT

The prospective amount of current that will flow in an electrical network when a short circuit fault occurs is referred to as the fault level and it is an important parameter in the definition of power equipment capabilities. Network fault levels are increasing above the rating of some existing equipment due to the connection of distributed generation and changes in network topology.

ENW's Respond project¹ is trialling new methods of mitigating fault level issues as alternatives to expensive replacement of equipment. The Respond project is a Low Carbon Network Fund (LCNF) Tier 2 project, which is funded by the Low Carbon Innovation Fund. Comprehensive project information can be obtained from the Respond website.

The Respond project aims to demonstrate the use of three innovative fault level mitigation (FLM) techniques which have not been previously used by a Distribution Network Operator (DNO) in the UK, namely;

- IS Limiters (essentially a fast acting explosive fuse device which senses the fault current rise and reconfigures the circuit so as to reduce the fault current)
- Adaptive Protection (AP) (a system whereby one out of two transformers in a substation is rapidly disconnected so as to reduce the subsequent fault current so that by the time other breakers trip they will not see excessive current)
- Fault Current Limiting service (FCL service) (a system whereby an external customer's site that contains generators or motors that could act as a fault current feed is rapidly disconnected so as to reduce the subsequent fault current so that by the time other breakers trip they will not see excessive current)

1.3 REQUIREMENT FOR SAFETY JUSTIFICATION

The FLM techniques being trialled by the Respond project, including AP, can introduce changes to the way existing equipment is operated. A safety justification assesses the changes to provide a clear and comprehensive argument that the proposed application of each FLM technique is or is not acceptably safe.

The Respond project's safety justifications are required to satisfy the Successful Delivery Review Criteria, SDRC 9.3.8, as detailed below:

¹ <http://www.enwl.co.uk/respond/about-respond/what-is-respond->

Criteria	Evidence
Write Safety Case for each fault level mitigation technology deployed	Publish peer reviewed Safety Cases on the Respond project website by September 2018

The SDRC uses the term 'safety case'. The Health and Safety Executive (HSE) views a safety case as a document associated with a licensing requirement to do work, such as in the nuclear industry. The HSE review such safety cases and may grant approval. In these terms, a safety case is not necessary for the use of the Respond project's FLM techniques because the techniques are not licensed and HSE permission does not need to be granted. However, ENW are committed to safety and as part of their safety processes they will produce a safety justification for the approach and this is presented here in the form of a safety case even though it is not part of a licence requirement.

Safety justifications for the Respond project have been produced by WSP, independently from ENW, with input from and peer review by other DNO(s) and presented to HSE to demonstrate that a robust approach has been taken.

Three safety justifications will be prepared by WSP, one for each of the three FLM techniques being trialled by the Respond project, to assess their safety and compliance with Applicable Laws insofar as these Applicable Laws relate to health and safety (H&S Applicable Laws).

This safety justification report covers the Adaptive Protection (AP) FLM technique. This safety justification is concerned with the safety of people, including the general public, through operation and maintenance. It does not specifically address the other aspects of the lifecycle (e.g. the manufacture, storage and disposal of the devices) or other risk categories (environmental, asset, reputation, etc.). It does not address failure to supply (i.e. compliance with ENW's Electricity Distribution Licence) or the environmental impact of incorrect operation.

Is Limiter and FCL service FLM techniques will be addressed separately in subsequent reports.

1.4 SAFETY JUSTIFICATION PROJECT

Figure 1-1 depicts the tasks undertaken to complete the safety assessment project.

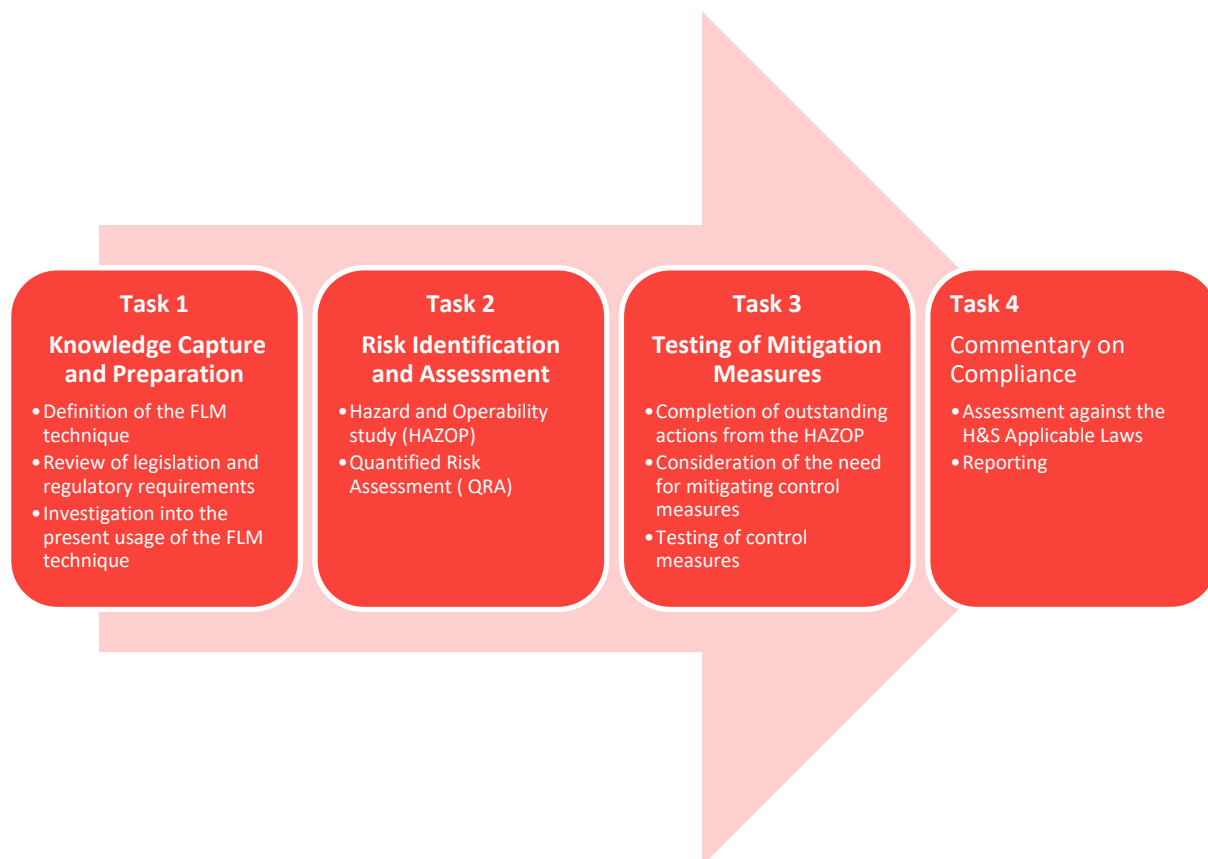


Figure 1-1 Respond Safety Justification Project Tasks

1.5 REPORT STRUCTURE

This report describes the process that has been followed to assess the safety of the use of Adaptive Protection in distribution networks and presents the results along with the conclusions and implications arising from those results. It comprises the following sections;

- Section 1 this introduction, provides the scope of the study and overview of the report structure;
- Section 2 describes the safety assessment methodology that has been followed;
- Section 3 defines Adaptive Protection for the purpose of this safety assessment;
- Section 4 explains the tolerability of risk framework and derivation of targets for this AP scheme
- Section 5 provides details of the review of applicable health and safety laws undertaken;
- Section 6 details results and findings of the hazard identification and quantified risk assessment with discussion of results, comparison with requirements and sensitivity to changes ;
- Section 7 draws out conclusions and the implications of the safety assessment; and suggests further steps in the development of an AP scheme.

Appendices present detail from analysis, including hazard list, QRA and safety requirements

2 SAFETY ASSESSMENT APPROACH

A review undertaken at the start of this study has not revealed evidence of previous applications of an FLM technique either very similar or identical to AP in the UK and elsewhere. Consequently no previous safety justification exists for this type of application and no precedent exists for reference or development.

However, the approach to assessment and justification of safety related systems generally is well understood and has been adopted for this study. This section describes the approach and the steps taken, as outlined in Figure 2-1, including wider management and supporting activities to ensure the quality and completeness of the final safety justification.

2.1 REVIEW OF LEGISLATION AND REGULATORY REQUIREMENTS

The first step of the assessment determines the legislative and regulatory framework applying to AP. This defines constraints and key requirements, which AP must comply with. The remaining steps in the safety assessment approach are tailored to address these requirements.

For most safety related applications the most relevant legislation is the Health and Safety at Work Act 1974² (HSW Act) which adopts a risk based approach, specifying that risks should be reduced So Far As Is Reasonably Practicable (SFAIRP). This essentially means weighing the risk presented by an AP installation against the trouble, time and money needed to control that risk. Thus, AP risks would be expected to be controlled SFAIRP.

Other legislation applies to the use of AP, such as the Electricity at Work Regulations (EAWR) 1989. This legislation includes requirements which are absolute rather than risk based. For example, EAWR Regulation 5 requires that no electrical equipment shall be put into use where its strength and capability may be exceeded in such a way as may give rise to danger. If AP is applied in a scenario where the fault current would exceed the circuit breaker rating, should the AP fail, then it could be interpreted that this is in contravention of Regulation 5.

Therefore, in conducting a review of the legislation and regulatory requirements, it is essential to consult with other industry stakeholders and particularly with HSE to establish their view as to the requirements arising from applicable H&S Laws and whether AP can meet those requirements.

Findings of the review of H&S applicable laws are presented and discussed in Section 5.

2.2 ESTABLISHING RISK CRITERIA

In order to determine whether the application of AP presents a 'Broadly Acceptable' or 'Tolerable' risk in accordance with legislation (SFAIRP and ALARP principles) it is necessary to establish appropriate risk tolerability criteria.

The study has investigated industry practice, consulted with ENW and used guidance from HSE's 'Reducing Risk Protecting People' publication to establish appropriate risk criteria for use with the Respond project.

Findings are presented and discussed in Section 4.

² <http://www.legislation.gov.uk/ukpga/1974/37/contents>

2.3 SAFETY ASSESSMENT METHOD

The safety justification considers safety, health and welfare issues associated with the use or failure of the AP technique and preparation of a critical risk assessment. It is based on the specific application of the AP technique being trialled and extrapolates to consider some options for implementation.

The overall process is summarised in Figure 2-1 below and each stage of the process is then briefly described.

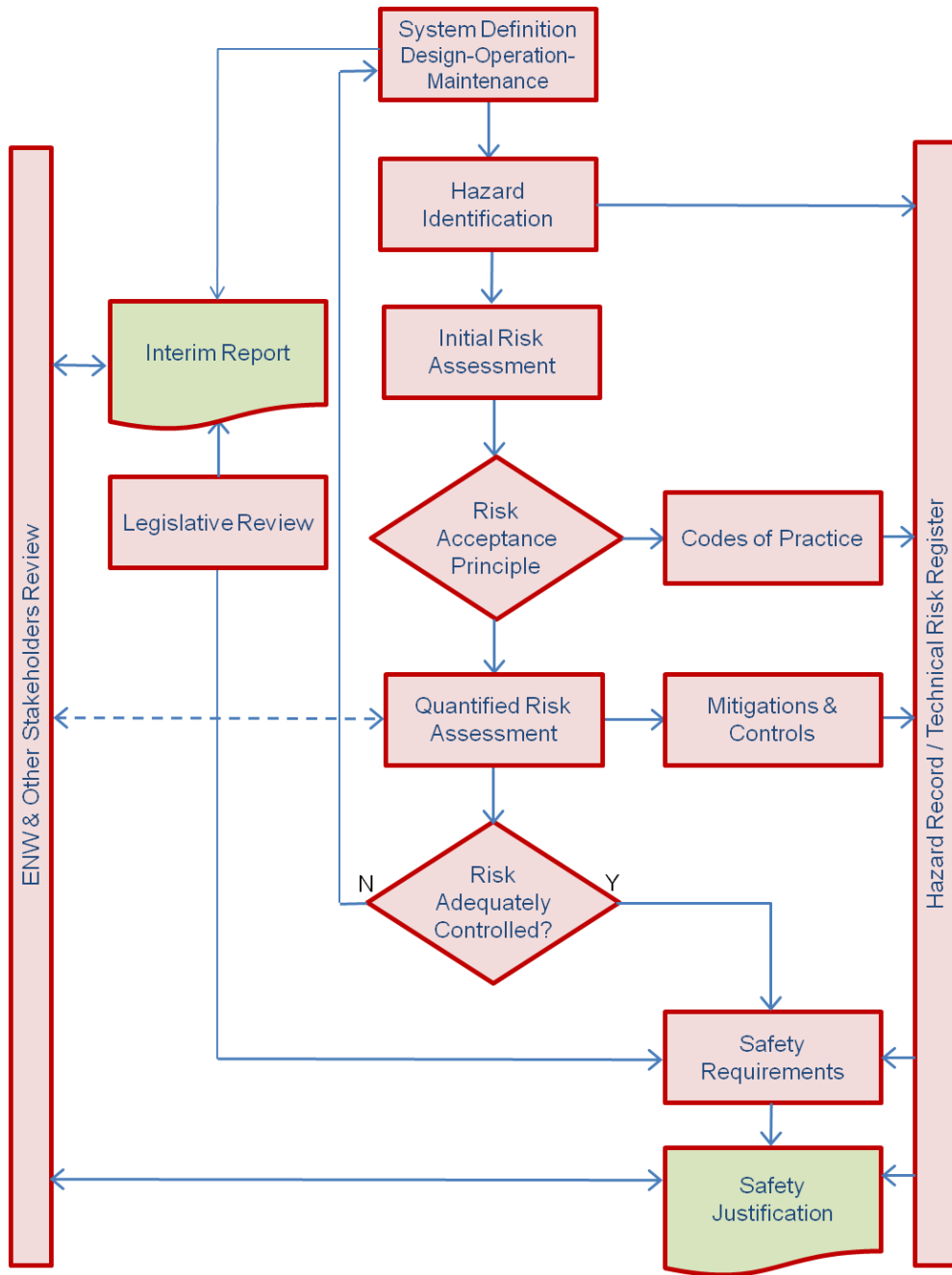


Figure 2-1 Respond Project Safety Assessment Process

2.4 SYSTEM DEFINITION

The system definition (Section 3) was based on a reference system with a number of alternatives. This formed the basis for the remainder of the analysis.

2.5 HAZARD IDENTIFICATION

A Hazard and Operability (HAZOP) workshop was conducted for AP based on the reference system described in Section 3. Identified hazards are presented in Section 6.1 with further detail in Appendix A.

2.6 INITIAL RISK ASSESSMENT

An initial risk assessment was conducted during the HAZOP and was based on the engineering judgement of those present regarding frequency and consequence of the hazards.

2.7 RISK ASSESSMENT PRINCIPLE

Where a particular risk can be controlled purely by adherence to existing standards or regulations the “code of practice” principle was used. Where such a code of practice did not exist the Quantified Risk Assessment (QRA) principle was used.

2.8 CODES OF PRACTICE

Where codes of practice were applicable they were identified and conformance to them became the justification for safety.

2.9 QUANTIFIED RISK ASSESSMENT

Risk associated with some hazards could not be satisfactorily controlled through the application of codes of practice. Therefore in these cases a quantified risk assessment (QRA) has been undertaken. The QRA has determined where further control measures have been required to satisfactorily reduce that risk. The QRA and findings are presented and discussed in Sections 6.2 to 6.7 with supporting calculations at Appendix B.

2.10 SAFETY REQUIREMENTS

Results from the HAZOP and QRA and from review of the H&S applicable laws have determined safety requirements and conditions necessary for the application of AP.

The safety justification includes statements and evidence to support where each safety requirement is achieved by the implementation of AP defined in Section 3. The safety justification also suggests improvements to the defined AP where this is necessary to achieve a safety requirement.

Safety requirements arising from the HAZOP and QRA are discussed in Section 6.8 and presented in Appendix C.

2.11 PROJECT SAFETY ORGANISATION

The project safety organisation depicts ENW’s role as owner of the safety justification, WSP as independent producer of the safety justification and the involvement of other stakeholders in the consultation and review process, as shown in Figure 2-2.

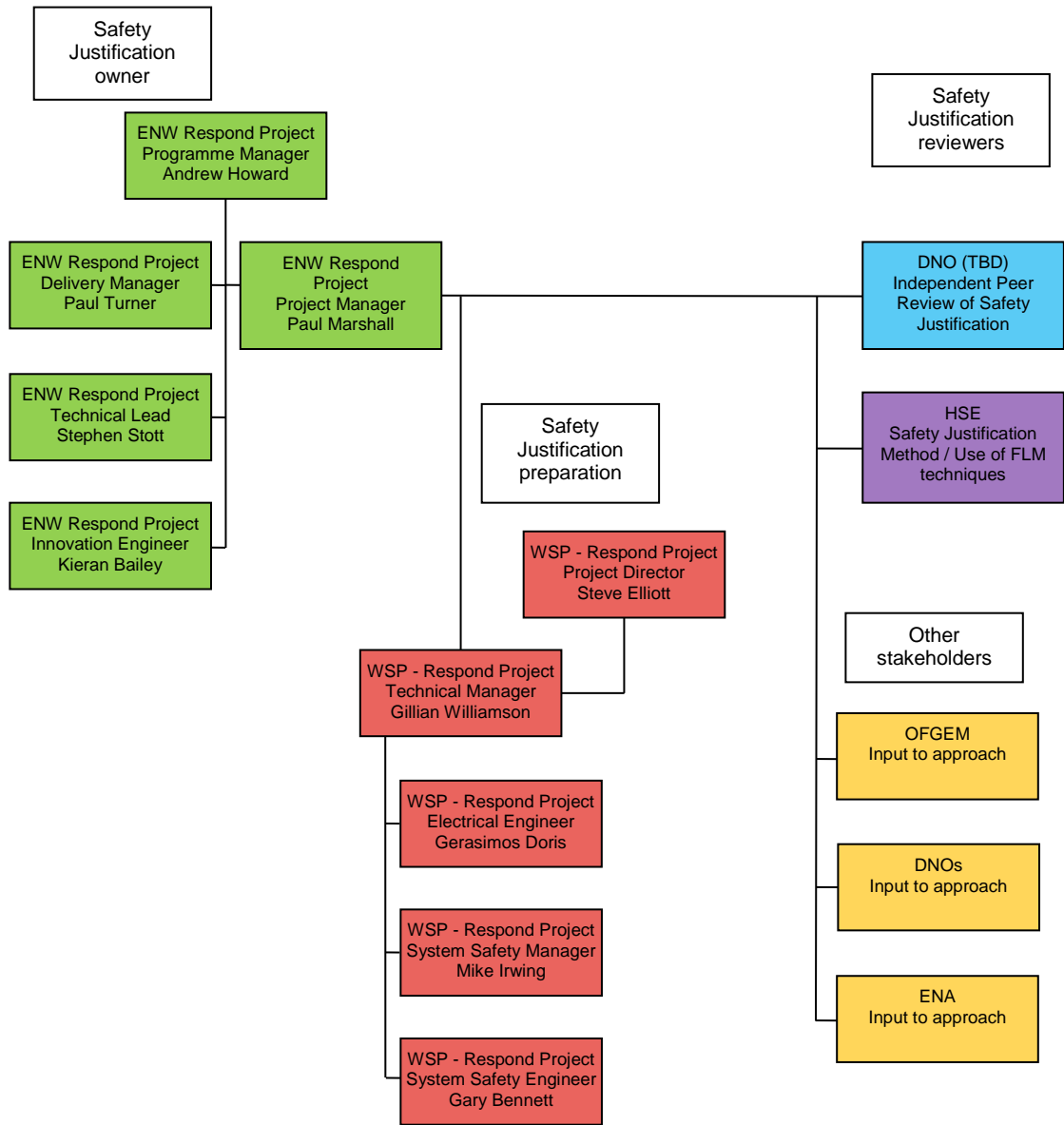


Figure 2-2 Safety Justification delivery and responsibility organisation

2.12 MANAGEMENT, REVIEW AND APPROVAL

The study has been undertaken in stages with interim findings being presented, documented and reviewed incrementally to ensure quality and validity of input data, assumptions and findings and to maintain focus on objectives.

Key review points included:

- An interim report presenting: a definition of a representative application of the AP technique based on a trial site installation; H&S Applicable Legislation review findings
- HAZOP workshop output
- Meeting with HSE
- Quantified Risk Assessment presentation to ENW at a meeting on 22nd January 2018
- ENW review of Safety Justification report

In addition, it is anticipated that an independent peer review will be conducted by another UK DNO having knowledge of and involvement in similar projects.

3 ADAPTIVE PROTECTION

3.1 INTRODUCTION

Details of AP as it will be installed and operated when applied as part of business as usual are given in this section for the purposes of the safety justification. It was important to describe how AP will be realised and will function in order that the potential hazards relating to the specific conditions could be established, evaluated and mitigated as required. This safety justification relates to the definition of AP given here.

It should be noted that the realisation of AP described may be marginally different than the installation for the Respond trials because of slightly different requirements. Fault levels do not exceed the equipment's rating at the trial sites and therefore there was no need for a safety case before the trial commenced.

AP is being trialled at five 11kV (or 6.6kV) and two 33kV substations. It has been concluded through these Respond trials that the operational issues associated with application of AP at 33kV mean that is unlikely to be pursued beyond the trial. Consequently AP is defined here for application at 11kV (6.6kV) only as there is no need to undertake a safety assessment for the application of AP at 33kV.

A Fault Level Assessment Tool (FLAT) incorporated into ENW's Network Management System has been developed as part of the Respond project. It assesses the network fault levels and has been considered as a method to control the enablement of the FLM techniques. However, it has been concluded based on the trial findings that the FLAT will not form part of the business as usual approach for the application of AP initially. Therefore, this definition of AP does not include FLAT functionality and it is taken to be permanently enabled for the purposes of this assessment. This safety assessment would need to be reviewed should enablement via the FLAT be subsequently incorporated into AP.

3.2 DEFINITION

3.2.1 Installation

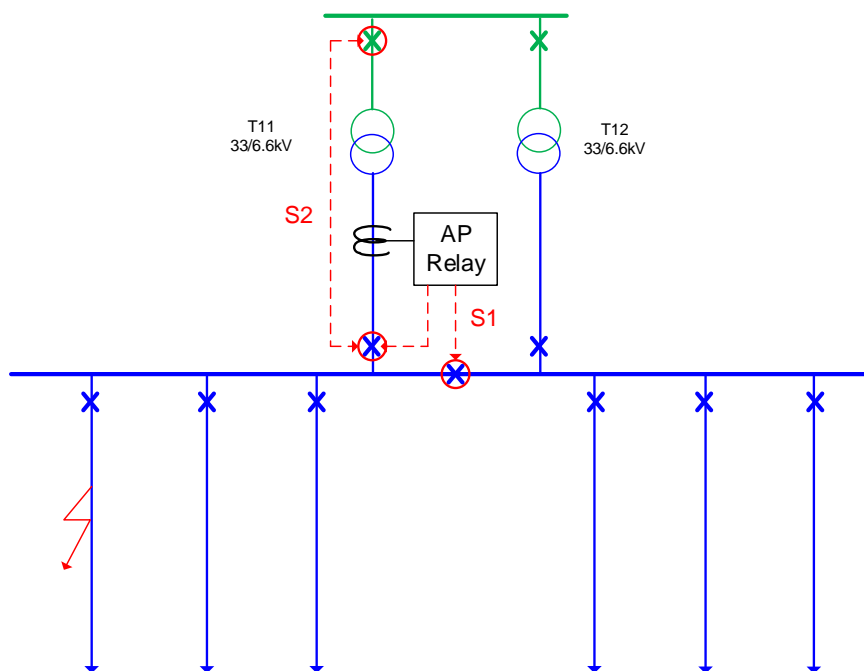
With AP the network is reconfigured to reduce the fault current before the circuit breaker is opened to clear the fault as normal. The re-sequencing of the circuit breakers is achieved by retrofitting new protection into existing substations.

The standard configurations for the application of AP for radial feeders and closed ring networks are shown in Figure 3-1 and Figure 3-2, respectively.

Table 3-1 presents the main parameters associated with the installation of AP.

Table 3-1 Adaptive Protection parameters

ADAPTIVE PROTECTION PARAMETERS	
Voltage	11kV (6.6kV)
Network Configuration	Two-transformer sites Radial and simple ring topologies (fixed, i.e. not changing with time) Solidly and impedance earthed 11(6.6)kV systems
Equipment	Adaptive Protection Relay Interposing current transformers (IPCT) on each phase of the LV sides of the two incoming transformers Standard hard wiring between the relay and circuit breakers
Relay Type	Modern programmable numeric type offering two stages of action Relay offers failure indicators For example AREVA P145 overcurrent and earth fault numeric relay
Installation	Inside a substation of standard construction
Enablement	Adaptive Protection permanently enabled



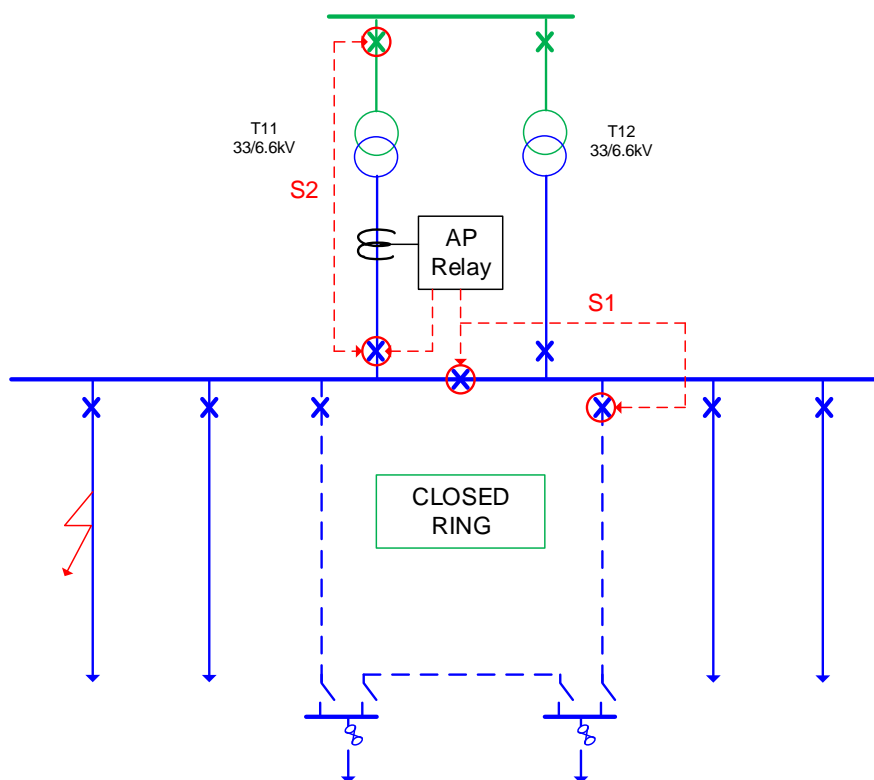
Method 1 – Radial Feeders

Stage 1 (S1) – Trips the 6.6kV bus coupler CB.

If S1 fails,

Stage 2 (S2) – Trips Transformer LV and HV CB.

Figure 3-1 Standard Adaptive Protection – Radial Feeders



Method 2 – Closed Ring

Stage 1 (S1) – Trips one of the ring CBs and the 6.6kV bus coupler CB.

If S1 fails,
Stage 2 (S2) – Trips Transformer LV and HV CB.

Figure 3-2 Standard Adaptive Protection – Closed Ring

3.2.2 Operation

The AP relay offers two stages of operation; the second stage operates automatically if the circuit breaker tripped by the first stage fails to open within 200ms.

In the radial feeders case, the AP relay trips the bus coupler on the 11(6.6)kV busbar. Each bus section is then only supplied by one transformer and the fault contribution from upstream is reduced, resulting in less fault current flowing to a fault in the downstream network. If the stage 1 action fails, then the second stage of the AP relay action trips the transformer LV circuit breaker and also the associated transformer HV circuit breaker where required by the network configuration. The network reverts from being supplied by two transformers in parallel to being supplied by one transformer and the fault contribution from the upstream system is reduced accordingly.

For ring circuits, the AP relay trips the bus coupler and one of the ring feeder circuit breakers. Opening one of the ring circuit breakers means that the ring no longer provides a parallel path between the busbar sections. Each bus section is then only supplied by one transformer and the fault contribution from upstream is reduced, resulting in less fault current flowing to a fault in the

downstream network. If the stage 1 action fails, then the second stage of the AP relay action trips the transformer LV circuit breaker and also the associated transformer HV circuit breaker where required by the network configuration. The network reverts from being supplied by two transformers in parallel to being supplied by one transformer and the fault contribution from the upstream system is reduced accordingly.

Switching at the HV side of the transformer may not be a local circuit breaker, but rather a remote circuit breaker via monitored remote intertripping.

A current transformer (CT) is installed on the LV side of one of the two 33/11(6.6)kV transformers which provide the supplies from the upstream system. It measures part of the current flowing from the upstream system and its output is fed into an AP relay which issues an instantaneous (without intentional delay) trip signal to the circuit breaker if a fault is detected based upon a programmable predetermined threshold. This predetermined value is set to cover the majority of multiphase faults on the 11(6.6)kV system, avoiding the risk of tripping for a single phase to earth fault or for load.

AP is realised within the incomer circuit breaker relay and operates without delay and in advance of the existing protection relays. All existing relay settings are not altered by the installation of AP.

ENW 11(6.6)kV networks are resistively earthed, however some GB DNOs solidly earth their 11(6.6)kV networks. Given these circumstances, a single phase to earth fault may be larger in magnitude than some multiphase faults. Consequently, the DNO would be required to adjust the AP overcurrent settings to match the fault level for a chosen level of multiphase faults and avoid against tripping for load current without trying to segregate against operation for earth faults.

Certain prerequisites need to be fulfilled in order for an AP relay to operate. These include:

- a) A 110V DC supply to power up the AP relay,
- b) The self-checking process in the AP relay confirms it is in a 'healthy' condition,
- c) The onsite AP ON/OFF switch is in the 'ON' position,
- d) The telecontrol (SCADA) AP IN/OUT latching interposing relay is in the 'IN' state,
- e) All local site topology conditions are confirmed to be correct by the AP relay i.e. T11 transformer, T12 transformer and bus-section 11(6.6)kV circuit breakers are all closed. Blocking logic is used within the AP relay to ensure that it does not trip the bus section or switch out a transformer if the one transformer is already switched out.

If any of the above mentioned prerequisites change, then the requirement for AP should be removed, possibly automatically, by tripping the Bus Section and/or Transformer circuit breakers so that fault currents are reduced

The AP relay has a self-monitoring function which issues an alarm reflected in a warning in the network control room should the relay fail.

3.2.3 Enhanced Protection with Redundancy

- 1oo1: The protection scheme described above uses a single relay and a single CT on each phase to sense the current. Such a scheme would cease to operate if a single component failed, known as a one out of one (1oo1) configuration.
- 1oo2: If a higher level of integrity was required then more redundancy could be incorporated by duplicating essential elements like the CT and the AP relay. This would be a one out of two (1oo2) configuration because it would continue operating with one of the two components failing.

A detailed design of this type does not exist at the time of writing this report but for the purposes of this safety justification it has been envisaged that it could be developed.

3.2.4 Network Conditions

AP will only be employed in networks when the following network conditions are met:

- i. The maximum prospective fault flow is within the peak make and break fault ratings of the bus section circuit breaker. (see safety requirement 28)
- ii. The maximum prospective fault flow is within the peak make and break ratings of the transformer circuit breakers. (see safety requirement 27)
- iii. The maximum prospective peak (asymmetrical) fault current flow that will be seen with AP protection installed and working is within the instantaneous fault withstand rating and thermal rating of the substation busbars and all circuit breakers, including the feeder circuit breakers, i.e. they can withstand the prospective fault current until AP Stage 2 operates. (See Safety requirements 3, 4, 11, 12)
- iv. The maximum prospective peak (asymmetrical) fault current flow that will be seen with AP protection installed and working is within the instantaneous fault withstand rating and thermal rating of the feeder cables and/or OHL, i.e. they can withstand the prospective fault current until AP Stage 2 operates. (see safety requirements 8, 9, 24, 25)
- v. It should be possible to reduce the fault current to within ratings by upstream switching in the event that circuit breaker control supplies are lost within the substation. (See Safety requirement 17)
- vi. The maximum prospective fault current even if AP fails is within the rating of existing customer switchgear on any feeder or the fault level at a customers' site is equal to or less than the design fault level (See Safety requirement 23)

3.2.5 Maintenance

Existing maintenance procedures and scheduling for two-transformer sites such as Denton West have been assumed to be in use.

3.3 EXISTING USAGE

Previous and existing use of the AP technique would be a useful source of information for producing a safety justification for this ENW application. WSP therefore performed a thorough search regarding existing applications which concluded that this specific concept is unique.

In the UK two related techniques have been identified, presented below for completeness, but no information relevant to this present application could be determined:

- A similar approach of tripping generators for a different reason was identified and is presented below. As mentioned earlier, ENW Adaptive Protection reduces fault current by reconfiguring the network so that less fault current flows from the upstream system in order to avoid exceeding the rating limits of protective equipment (circuit breakers).

Although not exactly the same, National Grid's System to Generator Operational Intertrip balancing service³ is along the same lines. National Grid operates 'a *Balancing Service of automatic tripping of the user's circuit breaker(s) resulting in the tripping of BM Unit(s) or (where relevant) Generating Unit(s) comprised in a BM Unit to prevent abnormal system conditions occurring, such as over-voltage, overload, system instability etc. after the tripping of other circuit breakers following power system fault(s)*'⁴. Circuits are prevented from exceeding their thermal limits under abnormal conditions, rather than fault conditions as is the case for AP.

- In addition, another concept that seems to be quite similar but from a different perspective is the System Integrity Protection Scheme (SIPS). This has been installed in the UK in 2008 and more specifically on the interconnection between Scottish Power and National Grid (Anglo-Scottish boundary). Within this framework, depending on predefined criteria, a trip command is selectively issued to Scottish Power generating units in less than 20ms in response to faults on the cross-boundary circuits.

According to the results of an internet based search, there are no identified international cases of the AP technique.

3.4 REFERENCE SYSTEM

Although AP is being trialled at multiple sites and will be applied in unknown locations as part of business as usual, the safety assessment takes as a starting point the installation on a single site agreed with ENW. This approach has been adopted because it is considered that the development of the safety justification benefits from basing it on a specific installation. Using a specific installation allows all hazards to be visualised and the sensitivities of the installation to be considered. The process aims to identify the "worst credible case" examples and indicate the safety margins so that, as explained later in this report, the safety justification has been generalized to a wide range of potential applications.

The reference case for the basis of the safety assessment was chosen to be a two-transformer site at Denton West.

The site's single line diagram is illustrated on Figure 3-3 as based on information given in ENW's Long Term Development statement⁵.

³ <http://www2.nationalgrid.com/uk/services/balancing-services/system-security/intertrips/>

⁴ www2.nationalgrid.com/WorkArea/DownloadAsset.aspx?id=15308

⁵ <https://www.enwl.co.uk/secure-area/ltds-document-library>

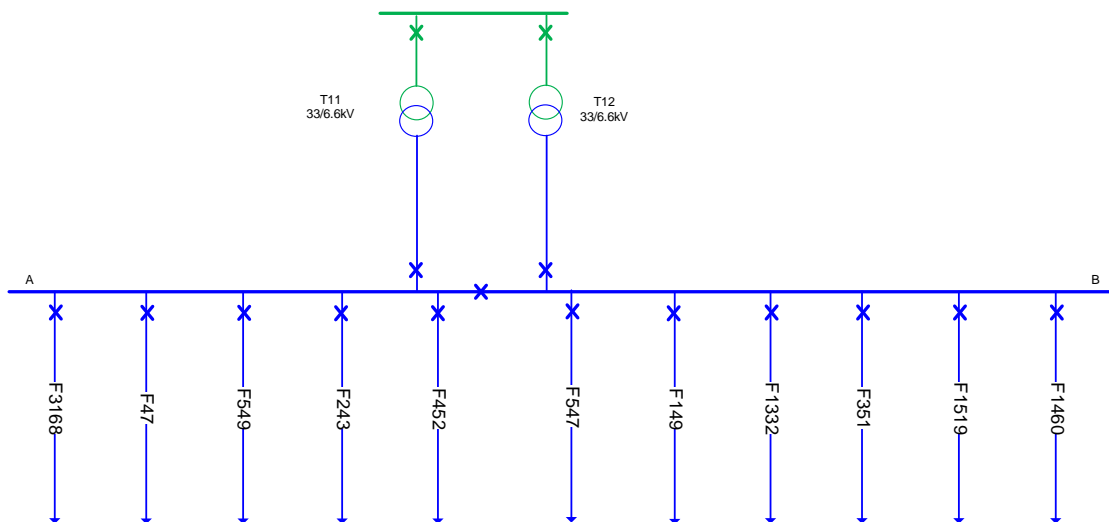
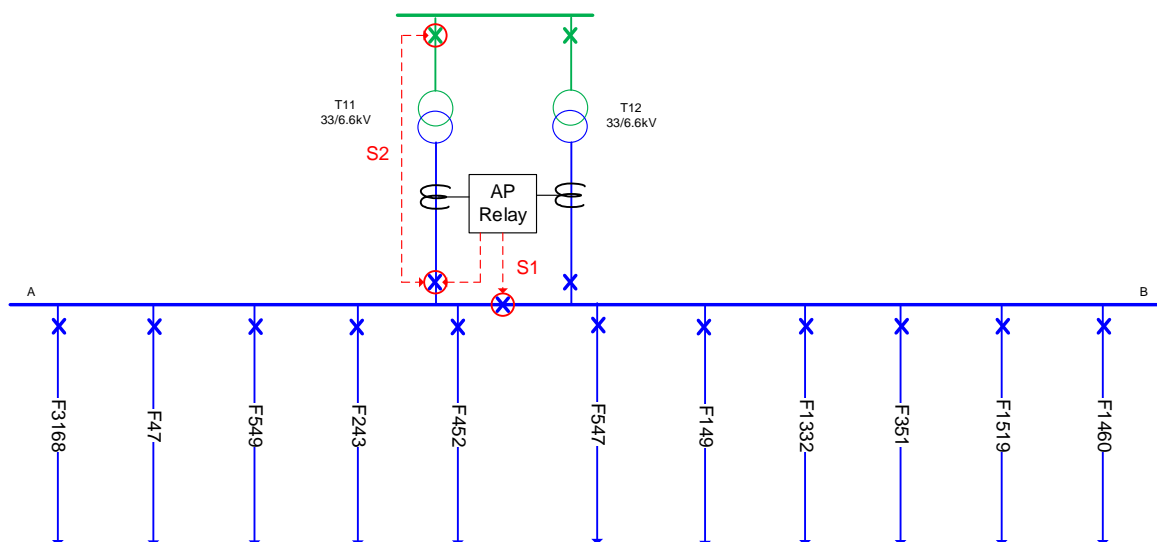


Figure 3-3 Denton West – single line diagram

AP has been implemented at Denton West as shown in Figure 3-4 as part of the Respond trial.



Radial Feeders method

- Stage 1 (S1) – Trips the 6.6kV bus section CB.
- If S1 fails then
- Stage 2 (S2) – Trips Transformer LV and HV CB

Figure 3-4 Adaptive Protection – Denton West configuration

4 TOLERABILITY OF RISK FRAMEWORK

The standard framework for tolerability of risk is explained in the HSE publication Reducing Risks Protecting People (R2P2)⁶.

R2P2 places risk into one of three regions: 'Unacceptable', 'Tolerable' and 'Broadly Acceptable'. These are depicted in Figure 4-1. As explained in Section 2.1 it is normally acceptable if risks in the tolerable region are reduced SFAIRP. However, in the case of AP, because it arguably contravenes Regulation 5, risks would need to be reduced to the "Broadly Acceptable" level.

Guidance in R2P2 has been used to determine the boundaries between the different regions.

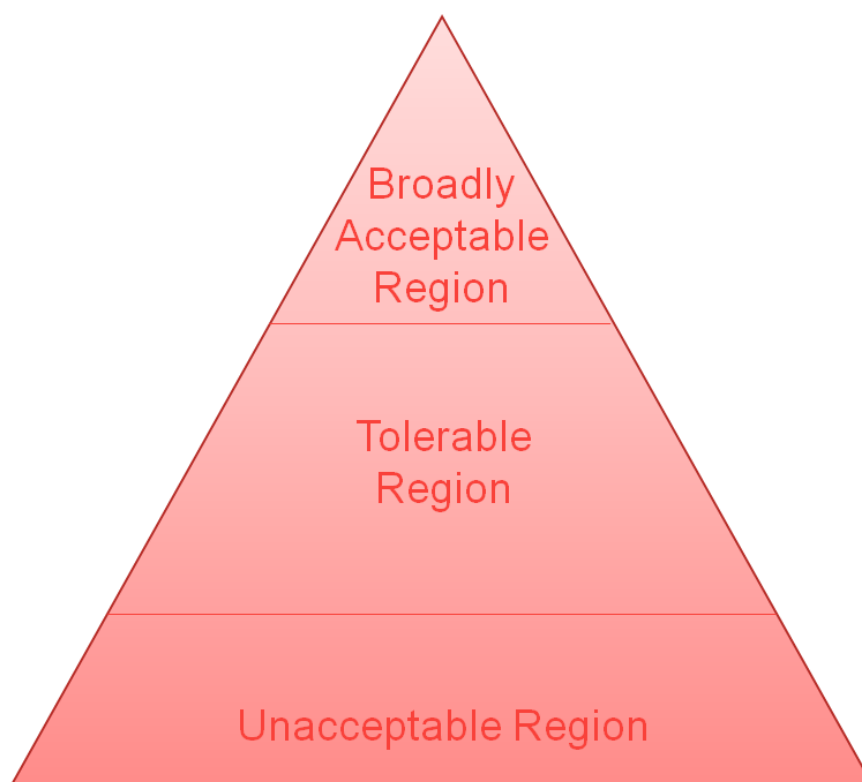


Figure 4-1 HSE framework for the Tolerability of Risk

The R2P2 guidance presents an upper tolerability limit for risk of death for an individual worker at 10^{-3} per annum and for an individual member of the public at 10^{-4} per annum.

The guidance also states that an individual risk of death at 10^{-6} per annum for both workers and the public corresponds to a very low level of risk and should be used as a guideline for the boundary between the 'Broadly Acceptable' and 'Tolerable' regions. The R2P2 tolerability limits for risk of death have been considered in the development of a risk framework for the Respond project to assess the use of each of the three FLM techniques (Adaptive Protection, Is Limiter and

⁶ <http://www.hse.gov.uk/risk/theory/r2p2.pdf>

Fault Current Limiting Service) on the ENW electricity distribution network. A risk matrix for workers is presented in Table 4-1 and a risk matrix for the public is presented in Table 4-2 and these represent the summation of risk across ENW from Respond schemes on a 'per hazard' basis. The individual risk is the probability for an exposed individual that they personally are killed or injured. Therefore, it is not the risk of a fatal accident but the risk to a specific individual being killed in that accident. For example if there is one fatal accident that kills a substation worker per year and there are 50 substation workers the individual risk is 1 in 50 years.

The R2P2 boundary values correspond to all of the risks faced by workers and the public, whilst the use of AP is only one of these risks. Consequently, the HSE guidance has been calibrated for the specific hazards due to the use of AP and the resulting boundary conditions are shown in Figure 4-2 for a single substation site.

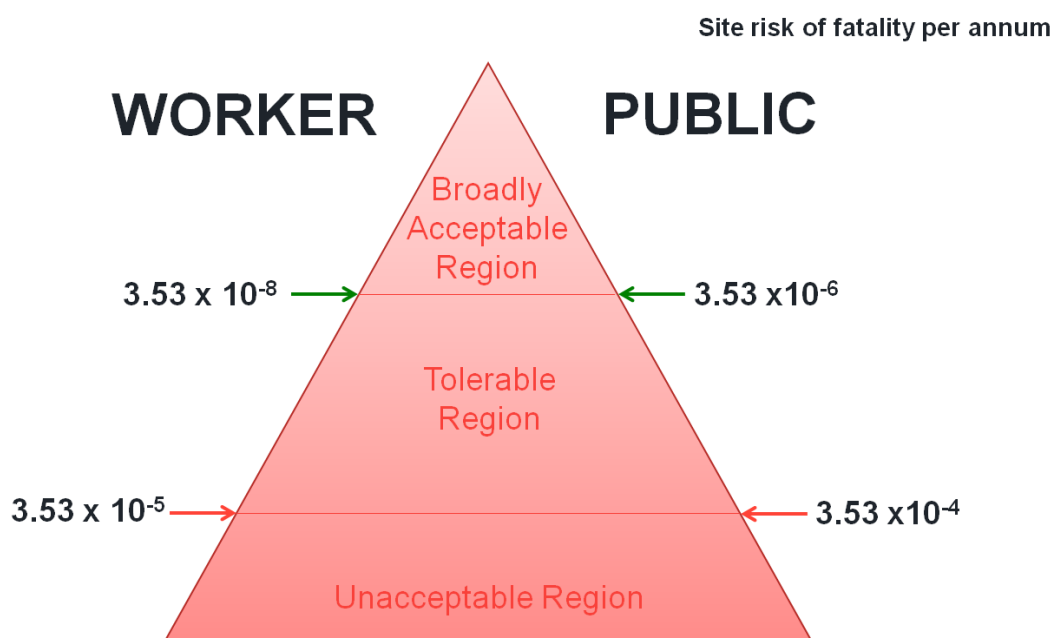


Figure 4-2 Specific Boundary values for RESPOND Project

These values can also be used as the basis for a matrix characterising the tolerability of risk presented by Respond hazards for workers (Table 4-1) and for the public (Table 4.2)

Table 4-1 Risk Matrix (per hazard) - Workers

SEVERITY	FREQUENCY (per annum)					
	6 Frequent > 10 ⁻¹	5 Likely > 10 ⁻² <=10 ⁻¹	4 Occasional > 10 ⁻³ <=10 ⁻²	3 Infrequent > 10 ⁻⁴ <=10 ⁻³	2 Remote > 10 ⁻⁵ <=10 ⁻⁴	1 Highly improbable > 10 ⁻⁶ <=10 ⁻⁵
5 Serious	Unacceptable	Unacceptable	Unacceptable	Unacceptable	Tolerable	Tolerable
4 Significant	Unacceptable	Unacceptable	Unacceptable	Tolerable	Tolerable	Tolerable
3 Moderate	Unacceptable	Unacceptable	Tolerable	Tolerable	Broadly acceptable	Broadly acceptable
2 Minor	Unacceptable	Tolerable	Tolerable	Broadly acceptable	Broadly acceptable	Broadly acceptable
1 Negligible	Tolerable	Tolerable	Broadly acceptable	Broadly acceptable	Broadly acceptable	Broadly acceptable

Table 4-2 Risk Matrix (per hazard) – Public

SEVERITY	FREQUENCY (per annum)					
	6 Frequent > 10 ⁻¹	5 Likely > 10 ⁻² <=10 ⁻¹	4 Occasional > 10 ⁻³ <=10 ⁻²	3 Infrequent > 10 ⁻⁴ <=10 ⁻³	2 Remote > 10 ⁻⁵ <=10 ⁻⁴	1 Highly improbable <=10 ⁻⁵
5 Serious	Unacceptable	Unacceptable	Unacceptable	Tolerable	Tolerable	Broadly acceptable
4 Significant	Unacceptable	Unacceptable	Tolerable	Tolerable	Broadly acceptable	Broadly acceptable
3 Moderate	Unacceptable	Tolerable	Tolerable	Broadly acceptable	Broadly acceptable	Broadly acceptable
2 Minor	Tolerable	Tolerable	Broadly acceptable	Broadly acceptable	Broadly acceptable	Broadly acceptable
1 Negligible	Tolerable	Broadly acceptable	Broadly acceptable	Broadly acceptable	Broadly acceptable	Broadly acceptable

The consequence classifications (severity) used in the Respond risk matrices are defined in Table 4-3. They are based upon the safety descriptors from a risk appetite framework used by ENW to qualitatively assess and manage risks in key areas of its business including safety.

Table 4-3 Consequence classifications

LEVEL	CONSEQUENCE	SAFETY/HEALTH DESCRIPTOR
1	Negligible	Slight injury not requiring treatment.
2	Minor	First aid / medical treatment is required.
3	Moderate	Time losing injury / health impact results.
4	Significant	A fatality / fatal occupational disease occurs or multiple Moderate injuries.
5	Serious	Multiple fatalities / fatal occupational diseases occur.

Each risk matrix has been calibrated for the Respond project to account for the expected hazards, at-risk population and contribution to the overall ENW risk profile using the following equations for the upper limit of tolerable risk, with parameters defined in Table 4-4. For the purposes of this calibration it was judged reasonable that if Respond was widely adopted it may constitute up to 2% of an overall workers risk. It was also assessed that Respond would introduce approximately 10 hazards based on the initial hazard identification.

Worker fatality (per Respond hazard) per annum $R_{WHT} = R_{IWT} \times P_{WRE} \times C_{PR} / H$

- Public fatality (per Respond hazard) per annum $R_{PHT} = R_{IPT} \times P_{PRE} \times C_{PR} / H$

Table 4-4 Risk matrix calibration

PARAMETER	VALUE	DESCRIPTION
R_{IWT}	10 ⁻³ per annum	Upper limit of tolerability for risk of death of individual worker per annum.
P_{WRE}	500	Worker population exposed to Respond hazards, assuming ENW/customer workforce of 2000 of which 25% operates in vicinity of switchgear.
C_{PR}	0.02	Contribution of Respond risk as proportion of overall ENW risk (i.e. 2%).
H	10	Estimated number of hazards associated with Respond project fault level mitigation techniques.
R_{WHT}	10 ⁻³ per annum per hazard	Upper limit of tolerability for risk of death from single hazard associated with Respond project, calculated using equation $R_{IWT} \times P_{WRE} \times C_{PR} / H$
R_{IPT}	10 ⁻⁴ per annum	Upper limit of tolerability for risk of death of individual member of the public per annum.
P_{PRE}	50,000	Public population exposed to Respond hazards, assuming population density 0.0001 persons per m ² in risk zone.
R_{PHT}	10 ⁻² per annum per hazard	Upper limit of tolerability for risk of death from single hazard

PARAMETER	VALUE	DESCRIPTION
		associated with Respond project, calculated using equation $R_{IPT} \times P_{PRE} \times C_{PR} / H$

Separately, the Energy Networks Association (ENA) has published guidance in its SHE Standard 07 Model Distribution Safety Rules (MDSR) which includes an approximation tool for risk assessment, refer to Figure 4-3. The derivation of the tool is not presented within the ENA standard, however a comparison has been undertaken between the tool and the risk tolerability matrices (Table 4-1 and Table 4-2) used in this document. There is a general correlation of results from both schemes although the risk matrices used in this document appear slightly more cautious than the ENA MDSR risk assessment scheme.

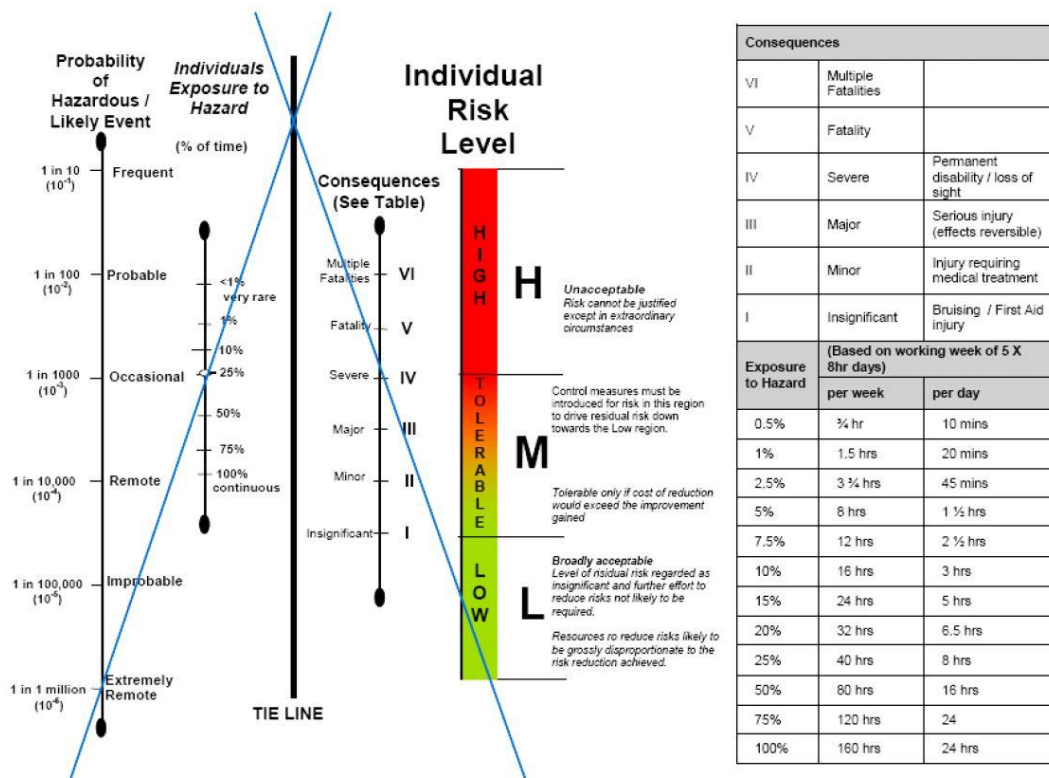


Figure 4-3 ENA risk assessment tool - extract from ENA SHE Standard 07 MDSR

5 LEGISLATIVE REVIEW

5.1 LEGISLATIVE FRAMEWORK

A review was conducted of H&S Applicable Laws and supplementary guidance relating to the implementation of an Adaptive Protective scheme in the UK. The review included:

- Health and Safety Work etc. Act 1974 (HSW Act)
- Management of Health and Safety at Work Regulations 1999
- Electricity at Work Regulations 1989 (EAW Regulations)
- EAW Regulations 1989 Guidance on Regulations HSR25 2015
- Electricity at Work: Safe Working Practices, HSG85, 2013
- Electricity Safety, Quality and Continuity Regulations 2002 (ESQC Regulations) with Amendments 2006 and 2009

Where significant requirements have been identified as applicable to changes introduced by AP to the DNO assets and operations, these have been included in Appendix D.

5.2 DISCUSSION OF REQUIREMENTS

For safety related applications, such as the AP scheme, the most relevant general legislation is the HSW Act which specifies that risks of injury associated with an undertaking shall be reduced 'So Far As Is Reasonably Practicable' (SFAIRP).

Similarly the ESQC Regulations, particularly pertinent to the safety of design and implementation of an AP scheme, require that the associated risks of injury shall be reduced SFAIRP.

Requirements based on the SFAIRP principle are achievable by developing and implementing an AP scheme which is underpinned by a hazard identification and risk assessment process including demonstration that risks not 'Broadly Acceptable' are nevertheless 'Tolerable' and 'As Low As Reasonably Practical (ALARP)'.

The EAW Regulations, however, include three regulations conferring requirements upon an undertaking, such as the AP scheme, which are construed as absolute requirements:

- Regulation 5 - *"No electrical equipment shall be put into use where its strength and capability may be exceeded in such a way as may give rise to danger"*⁷
- Regulation 11 - *"Efficient means, suitably located, shall be provided for protecting from excess of current every part of a system as may be necessary to prevent danger."*
- Regulation 12 - *"Where necessary to prevent danger, suitable means (including, where appropriate, methods of identifying circuits) shall be available for: (a) cutting off the supply of electrical energy to any electrical equipment; and (b) the isolation of any electrical equipment."*

⁷ In the EAW Regulations "danger" means risk of injury

HSR25, HSE guidance on the EAW Regulations, is particularly relevant to the implementation of AP and provides clear interpretation of the meaning of the terms used in the regulations and of the purpose of each regulation.

HSR25 clause 58 states:

“If the requirement in a regulation is ‘absolute’, for example if the requirement is not qualified by the words ‘so far as is reasonably practicable’, the requirement must be met regardless of cost or any other consideration. Regulations making such absolute requirements are subject to the defence provision of regulation 29.”

Appendix D cites several extracts from the HSR25 guidance associated with Regulations 5, 11 and 12 where the extracts explain the relevant requirements and how the ‘absolute’ and ‘reasonably practicable’ terms apply.

Regulations which contain ‘absolute’ requirements are therefore unequivocal.

AP is intended for use in cases where fault levels would potentially exceed equipment capability. If AP was to be applied in a case where the fault current could exceed the circuit breaker rating then, should the AP fail, it may be interpreted as being in contravention of EAW Regulations 5, 11 and 12.

HSE expressed the view, when consulted about this specific point, that failure of AP would contravene these regulations and that the defence against prosecution, in accordance with Regulation 29 of the EAW Regulations, would be that a person or organisation (i.e. ENW) would need to prove that it had taken all reasonable steps and exercised due diligence to avoid commission of an offence against the Act. In the view of HSE this would be satisfied if any risks were shown to be “Broadly Acceptable” and hence the normal SFAIRP argument would not apply.

6 HAZARD IDENTIFICATION AND QUANTIFIED RISK ASSESSMENT

This section documents the hazards identified as associated with the AP scheme and presents the results of the risk assessment conducted to determine the level of risk presented by the scheme.

6.1 IDENTIFIED HAZARDS

The HAZOP exercise identified four hazards that represent a significant potential risk to workers on or close to the substations where AP is applied and to members of the public in close proximity to the affected substations or transmission cables. These are:

- a) Short circuit of the busbar in a substation resulting in excessive fault current
- b) Short circuit within a Circuit Breaker in the substation resulting in excessive fault current
- c) Short circuit of the feeder cables or something connected to these cables such that the feeder cable withstand current is exceeded
- d) Short circuit of the overhead line or something connected to the overhead line such that the overhead line withstand current is exceeded

For each of these hazards a quantified risk assessment has been conducted.

A further 19 hazards were identified which presented no significant change to the situation existing without AP applied. The complete list of hazards is included at Appendix A.

6.2 QRA METHODOLOGY

Event Tree has been used as the QRA methodology. This starts with the initiating event (e.g. feeder cable short circuit) and then considers how this can develop into a range of possible outcomes including fatality and other accident scenarios. In general the event tree for each hazard progresses with the AP failure resulting in an explosion and then with either a worker or a member of the public in critical proximity they are killed by the explosion.

By considering the frequency of the initiating event and the probabilities of each of the subsequent steps in the accident chain the overall frequency of accidents is calculated.

6.3 INPUT DATA

6.3.1 Frequency of Initiating Events

The frequency of each of the initiating events has been estimated using available data as summarised in Table 6.1.

Table 6-1 Frequency of initiating events

PARAMETER	VALUE	SOURCE
Short circuit within a circuit breaker	0.0022 per AP site per annum	Based on a failure rate for all circuit breaker faults from NAFIRS ⁸ , adjusted using values from the IEEE Gold Book for the proportion of failures that are short circuits and allowing for 10 circuit breakers on average per site.
Short circuit of the feeder cables	0.322 per AP site per annum	Based on a failure rate from NAFIRS data for ENW per 100km of cable and assuming (based on fault current estimates) that an excessive fault current could only arise due to a short circuit in the first 700m of cable and that on average there are 10 feeder cables per substation. It is assumed that all short circuits will develop from phase to earth to phase to phase before feeder CB operates.
Short circuit of the overhead line	0.4284 per AP site per annum	Based on a failure rate from NAFIRS data for ENW per 100km of overhead line and assuming (based on fault current estimates) that an excessive fault current could only arise due to a short circuit in the first 700m of overhead line and that on average there are 6 feeders per substation. It is assumed that all short circuits will develop from phase to earth to phase to phase before feeder CB operates.

6.3.2 Probability of AP Failure

It has been estimated that since the circuit breakers that are tripped by the relay are duplicated their failure rate is negligible (i.e. the probability of both CBs failing together is negligible) in comparison to the single relay for the 1oo1 configuration. For the 1oo2 configuration the relay is estimated using manufacturers data to have a failure rate approximately 20 times higher than the Circuit breaker failure rate based on NAFIRS data for ENW. Therefore the relay failure rate dominates the equation and, given the two relays used will be identical, this has been dominated by common cause failure where two identical items fail because they share the same endemic failure mechanism. The calculation takes account of the percentage of failures that are detected by the relay self diagnostic and flagged up to the operator for rectification (assumed within 8 hours) and those that are not detected. The undetected failures dominate the probability of failure on demand which has been estimated as 0.0042 for the 1oo1 solution and 0.000228 for the 1oo2 solution.

Table 6-2 AP failure input data

PARAMETER	VALUE	SOURCE
Relay Total failure Rate	0.042 per Relay per annum	Manufacturers data
Relay Undetected Failure Rate	0.0042 per Relay per annum	Conservative estimate that 90% of failures will be either detected by diagnostics or will cause a trip when it should not
Circuit Breaker Total failure rate	0.0022 per relay per annum	Based on failure rate from NAFIRS data for ENW
Circuit breaker failure to operate on demand	0.00022 per AP site per annum	From Gold Book failure mode data that 10% of failures are found on test or are failure to open

⁸ National Fault and Interruption Reporting Scheme

6.3.3 Probability of Worker Fatality

The probability of a worker fatality in the event of an explosion due to an initiating event has been estimated as 0.00001. This assumes that there is a procedure in place such that the network will be reconfigured to reduce fault level within equipment capabilities before a worker enters the substation. Given that these sites are unmanned the normal probability that a worker is in a substation has been estimated at 90 hours per year (i.e. 1% of the time) by the HAZID workshop team. Given the procedure of reconfiguration before a worker enters a site it is expected the probability of this procedure failing is 1 in 100. The probability that the worker is actually killed by the explosion resulting from AP failing has been estimated as 0.1. Together these assumptions lead to the overall probability of a worker being killed of $0.01 \times 0.01 \times 0.1 = 0.00001$.

6.3.4 Probability of Public Fatality

The probability of a member of the public being killed in the event of an explosion event is dependent on the specifics of the site. For the purposes of this analysis it has been assumed there are high, medium and low risk sites.

A high risk site has been defined as a site where the risk of public fatality is high (between 0.3 and 0.03 or 1 in 3 to 1 in 30). This means that people would need to be present a high percentage of the time and also that an explosion would need to present a risk to these people either because the substation itself collapses and the people are close enough to be killed by the collapse or because the feeder cable exploding is directly underneath a person and the ground or cable duct does not contain the explosion. The Event Tree analysis has assumed the geometric mean case (0.1) for high risk substations.

A medium risk site has been defined as a site where the risk of public fatality is medium (between 0.03 and 0.003 or 1 in 30 to 1 in 300). This means that people would need to be present a significant percentage of the time and also that an explosion would need to present a risk to these people either because the substation itself collapses and the people are close enough to be killed by the collapse or because the feeder cable exploding is directly underneath a person and the ground or cable duct does not contain the explosion. The Event Tree analysis has assumed the geometric mean case (0.01) for medium risk substations.

A low risk site has been defined where the risk of public fatality is low (less than 0.003 or 1 in 300). The Event tree analysis has assumed a value of 0.001 for low risk substations (geometric mean of 0.003 to 0.0003).

An example of a high risk site would be where there is a substation in a busy area (e.g. a shopping centre) and that site was not protected against explosions inside the substation or of the cable and the cable is not rated for the fault current that could occur if AP failed. In reality it is suspected that sites in this type of situation are likely to incorporate measures to protect against explosions because there are already possible causes of such explosions on these sites but this has to be allowed as a possibility.

An example of a medium risk site would be an urban site where the feeder cable runs under the pavement at a school entrance and could fail explosively on fault current and the failure is not contained. If it is estimated that people gather outside school gates around 2 hours per day (1 in 10) and that these people occupy 35m out of the possible 700m failure zone for the feeder cable (1 in 20). This gives an overall risk of 1 in 200 which is within the medium risk boundaries.

Another example of a medium risk site would be an urban site where a house is situated in the substation building collapse zone and substation is not blast proof. It is estimated that the risk that the building collapses on the side where the house is situated is 1 in 4 and the risk that the building is occupied at the time is 1 in 2 and then that the person(s) in the house are killed is 1 in 5. This gives a total risk of 1 in 40 which is medium risk.

6.4 QRA RESULTS

The Event Trees are presented in Appendix A and summarised in the Table below which compares the overall risk with the targets for 'Tolerable' and also 'Broadly Acceptable'. They are also shown graphically in Figure 6-1. It should be noted that the low risk category includes feeder cable substations and also those with overhead line feeders. These have slightly different risks. It has been assumed that no medium or high risk sites have overhead line feeders because these are only used in rural situations.

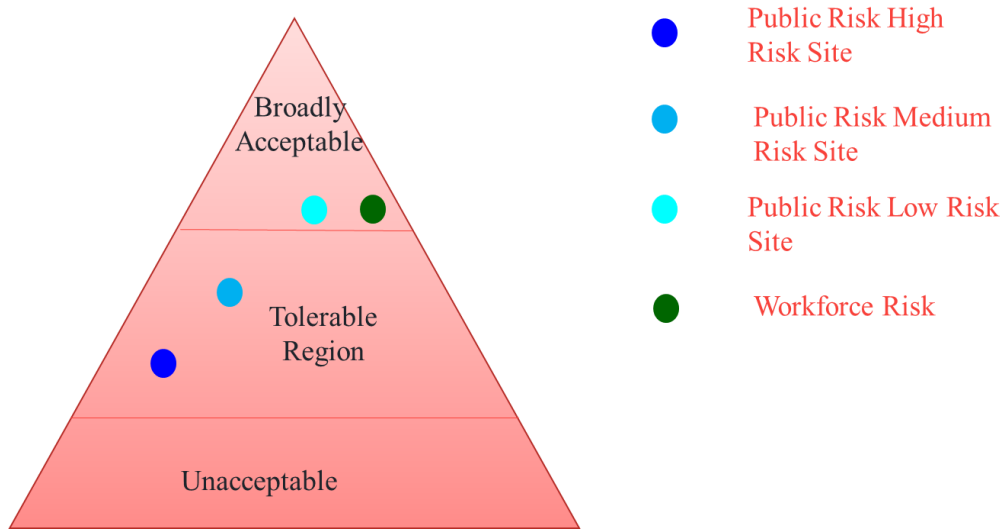


Figure 6-1 Respond AP Risks 1001 (no redundancy, SIL 2 system)

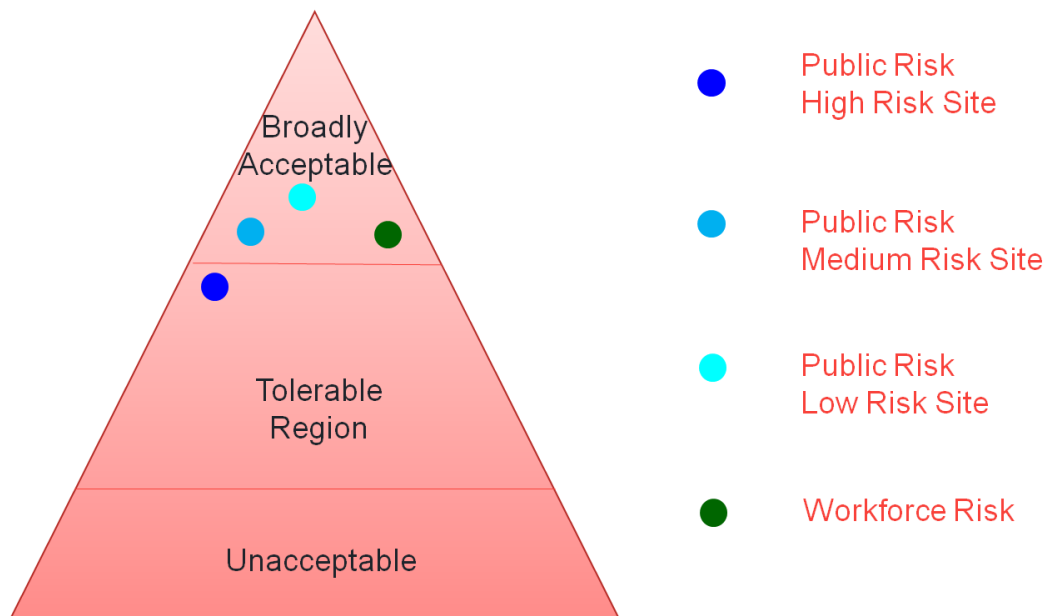


Figure 6-2 Respond AP Risks 1002 (with redundancy, SIL 3 system)

Table 6-3 QRA Results

Consequence	Frequency per site per annum	'Tolerable' upper limit per site per annum (all Respond hazards)	Meets 'Tolerable' upper limit?	'Broadly Acceptable' limit per site per annum	Meets 'Broadly Acceptable' limit?	Further risk reduction factor required for 'Broadly Acceptable'
Calculation using 1001 AP relays						
Public fatality High Risk	1.43x10 ⁻⁴	3.54 x10 ⁻⁴	Yes	3.54 x10 ⁻⁶	No	38.8
Public fatality Medium Risk	1.43 x10 ⁻⁵	3.54 x10 ⁻⁴	Yes	3.54 x10 ⁻⁶	No	3.9
Public fatality Low Risk (Overhead Line)	1.88 x10 ⁻⁶	3.54 x10 ⁻⁴	Yes	3.54E-06	Yes	
Public fatality Low Risk (Feeder Cable)	1.43 x10 ⁻⁶	3.54 x10 ⁻⁴	Yes	3.54 x10 ⁻⁶	Yes	
Workforce Fatality	1.66 x10 ⁻⁸	3.53 x10 ⁻⁵	Yes	3.53 x10 ⁻⁵	Yes	
Calculation using 1002 AP relays						
Public fatality High Risk	7.88 x10 ⁻⁶	3.54 x10 ⁻⁴	Yes	3.54 x10 ⁻⁶	No	2.1
Public fatality Medium Risk	7.88 x10 ⁻⁷	3.54 x10 ⁻⁴	Yes	3.54 x10 ⁻⁶	Yes	
Public fatality Low Risk (Overhead Line)	1.03 x10 ⁻⁷	3.54 x10 ⁻⁴	Yes	3.54 x10 ⁻⁶	Yes	
Public fatality Low Risk (Feeder Cable)	7.88 x10 ⁻⁸	3.54 x10 ⁻⁴	Yes	3.54 x10 ⁻⁶	Yes	
Workforce Fatality	1.82 x10 ⁻⁹	3.53 x10 ⁻⁵	Yes	3.53 x10 ⁻⁸	Yes	

6.5 DISCUSSION OF RESULTS

The QRA results indicate on the basis of the adopted methodology and all assumptions, that the requirement that risks should be reduced to the "Broadly Acceptable" level as advised by HSE is met for the 1001 case for low risk sites but not for medium or high risk sites.

The results shown in Table 6-2 indicate on the basis of the adopted methodology and all assumptions, that the requirement that risks should be reduced to the "Broadly Acceptable" level as advised by HSE is met for the 1001 AP solution for low risk sites and the 1002 redundant AP solution for medium risk sites. However, high risk sites could not safely be fitted with AP unless measures were taken to reduce the risk at those sites to make them medium risk.

6.6 SENSITIVITY ANALYSIS

The analysis in this report is based upon a number of estimates and assumptions which might be subject to challenge and review. Overall it is believed that the results are realistic or likely conservative because the failure rates are based on actual failure data, either for ENW or, in the case of the relays, from a relay manufacturer. It is estimated that the probability of a worker entering an AP site without it being reconfigured beforehand so as to reduce fault currents (which is part of the agreed procedures) is 1 in 100. Given that the worker would clearly be putting

himself at risk and that the industry understands the importance of correct operation to protect people it is felt that this is a reasonably conservative assumption. It is assumed that if there is a fault a circuit breaker or cable subject to current above its rating will fail in an explosive manner whilst in reality it is quite possible that it would actually withstand the increased current. It was also assumed that all faults in feeder cables or OHL would develop from phase to earth to phase to phase before the feeder CB operates, which is a clearly conservative assumption.

It should be noted that the margin between the estimated frequency of fatality and the broadly acceptable level is a factor of close to two in the worst case which gives further confidence that the recommendations made are robust.

6.7 IMPLICATIONS OF 1001 AND 1002 SOLUTIONS

The current analysis considers either 1001 or 1002 AP solutions. The 1001 solution does not employ a redundant relay and current sensors and is estimated to have a probability of failure on demand of 0.0042. Referring to the safety integrity level (SIL) classification scheme of the standard BS EN 61508⁹, this probability falls into the SIL 2 category and therefore to meet best practice the solution would need to be shown to meet the requirements of SIL 2 as defined in the standard. These requirements include architectural requirements and also requirements for the development lifecycle and for software. In the case where the software is already existing (as for a MICOM relay) it may be possible to use a “proven in use” argument rather than meeting the alternative detailed requirements of BS EN 61508. It may also be possible to use a “proven in use” argument for hardware to at least some extent. Conformance to SIL 2 would need to be demonstrated as part of the final 1001 solution development.

The 1002 solution uses redundant relays and current sensors and is estimated to have a probability of failure on demand of 0.000228. This probability falls into the SIL 3 category of BS EN 61508 and therefore to meet best practice the solution would need to be show to meet the requirements of SIL 3 as defined in BS EN 61508. These requirements include a similar range of requirements as described for SIL 2 applications. However, it should be noted that the requirements for SIL 3 are significantly more onerous than for SIL 2 and the formal demonstration of conformance to these requirements is not an insignificant task.

6.8 SAFETY REQUIREMENTS

The risk assessment has identified safeguards, controls and mitigation measures necessary to manage the level of risk associated with the implementation of the defined AP scheme. These become the safety requirements which the AP implementation must achieve to ensure control of the risk associated with each of the hazard scenarios and for the defined AP scheme to present a ‘Tolerable’ level of safety risk. Referring to the complete list of safety requirements presented in Appendix C, these include:

- a) Application conditions that must be satisfied before applying AP to a site, i.e. pre-requisites

SRs 2, 3, 4, 8, 9, 11, 12, 17, 23, 24, 25, 27, 28

- b) Safety function and performance measures necessary for the AP system, including safety integrity level

⁹ BS EN 61508: 2010, Functional safety of electrical/electronic/programmable electronic safety-related systems, Parts 1-7, BSI

SRs 1, 6, 13, 15, 18, 19, 20, 21, 22, 26

- c) Risk reduction measures for high risk sites to reduce risk to medium risk.

SR 7

- d) Implementation, operating and maintenance measures necessary to control safety risk of the AP scheme in use, including compliance with safety management systems, standards, procedures and codes of practice.

SRs 5, 10, 14, 16, 19, 20, 26

Following evidence from ENW that single phase faults can progress to become phase to phase faults SR21 which specifies that AP should be set so as not to trip on single phase faults may be ill advised. This is because if a single phase fault progresses to phase to phase it is possible that the feeder circuit breaker would start tripping on a single phase fault but by the time it actually trips would be subject to the higher current (above its rating) because the fault had progressed to a phase to phase fault and AP would not protect because it only starts to trip once the phase to phase fault has become established. This Safety requirement should therefore be reviewed.

It should be noted that the requirement that feeder circuit breakers and busbars can both withstand the fault currents up until the point where AP protection stage 2 has operated is particularly difficult to demonstrate compliance with. In particular, the specification for existing circuit breakers gives a 3 second through current rating that is the same as the maximum break current and therefore if the maximum break current is exceeded (which is the reason why AP would be employed in the first case) then this 3 second rating would be exceeded. The time for stage 2 of AP to operate is estimated to be 400ms and therefore in order to comply with the safety requirement the circuit breaker would need to be able to withstand the worst case fault current for up to 400ms. Whilst it is possible that the 3 second fault current is limited by thermal considerations and therefore a higher current could be withstood for 400ms there is no hard evidence that this is the case and such evidence would need to be established as part of the AP project. A similar argument would apply to the busbars.

6.9 NEXT STEPS

Tasks required to finalise this safety justification include:

- ENW request to an independent DNO such as UK Power Networks (UKPN) to conduct a formal review of this safety justification in order to increase stakeholder participation and strengthen the value of the report. Another DNO (UKPN) has already been briefed on the approach, methodology and findings of this AP safety justification and so may be a useful party to seek this further engagement from.
- ENW conduct a formal review of this safety justification to confirm that objectives have been achieved and to use as input to developing a plan for possible future implementation of an AP scheme.

The potential for a wider future development and implementation of an AP scheme is included in Section 7.2.

7 CONCLUSIONS

7.1 SUMMARY

This study has proposed a safety justification for implementation of the defined AP scheme within the ENW network.

The analysis has shown that, based on arguably conservative assumptions, it would be acceptable from a safety viewpoint to fit substations with an AP system provided that they are not high risk sites and that an AP in system 1oo1 configuration is used for low risk sites and 1oo2 configuration for high risk sites. The 1oo1 configuration would be required to meet the SIL2 requirements of BS EN 61508 and the 1oo2 configuration would need to meet SIL3.

Using recognised safety assessment processes, hazards associated with the AP scheme have been identified. Means of eliminating, controlling or mitigating the potential consequences of these hazards have been established. A quantified risk assessment has been performed which demonstrates the residual safety risk presented to workers and to members of the public by the defined scheme.

Four hazard scenarios associated with the implementation of the defined AP scheme have been determined to present the most significant risk. These include the potential for exploding feeder cables and fire and structural damage at substations, possibly causing injuries and fatality for workers and members of the public.

Safety requirements (further to those already in place for the existing network and operations) have been established by the risk assessment based on the detailed input data and assumptions. Achievement of these safety requirements would ensure control of the risk associated with each of these scenarios and the defined AP scheme would present a Tolerable safety risk. The safety requirements include:

- a) Application conditions that must be satisfied before applying AP to a site, i.e. pre-requisites
- b) Safety function and performance measures necessary for the AP system, including safety integrity level
- c) Implementation, operating and maintenance measures necessary to control safety risk of the AP scheme in use, including compliance with safety management systems, standards, procedures and codes of practice.

It should be noted that SR 21 has a potential safety risk and should be further investigated prior to application.

The study has also reviewed the requirements laid down by health and safety applicable legislation relevant to the defined AP scheme. This identified 'absolute' requirements of the EAW Regulations, specifically Regulations 5, 11 and 12 which, unlike other legislation requirements, are not satisfied by 'reasonably practicable' risk control measures and safety arguments. The EAW Regulations, Regulation 29, sets out the means for a legal defence in the event these 'absolute' regulations are breached.

This point has been discussed with HSE and a point of view offered by HSE was that provided a risk assessment had been performed which justified that the risk presented by the AP scheme was 'Broadly Acceptable' then this would support an ENW claim that it had taken sufficient steps to comply with the Regulations.

The study has therefore considered steps that could be taken by ENW to demonstrate that risks associated with the defined AP scheme are 'Broadly Acceptable' for all scenarios.

Introducing a 1oo2 configuration for the AP relay moves the residual risk for all but one scenario into the 'Broadly Acceptable' region. Further risk reduction measures would be required to protect the public at high risk sites, e.g. at a shopping centre.

By ensuring that substation structures and cable routes are able to contain the effects of explosion and fire at high risk sites, they would then become medium or low risk sites and the risk associated with the scenario would then become 'Broadly Acceptable'.

The study considered the robustness of the input data and assumptions and determined that some current data and assumptions could be over-pessimistic. Where a justification could be made to refine these then that may remove the need for the additional measures for substation structures and cable duct protection at high risk sites.

7.2 FURTHER DEVELOPMENT TO SUPPORT FUTURE IMPLEMENTATION

It is proposed that ENW requests an independent DNO such as UKPN to conduct a formal review of this safety justification in order to increase stakeholder participation and strengthen the value of the report. UKPN has already been briefed on the approach, methodology and findings of this AP safety justification and so may be a useful party to seek this further engagement from.

It is recommended that ENW conducts a formal review of this safety justification to confirm that objectives have been achieved and to use as input to developing a plan for possible future implementation of an AP scheme and incremental safety justifications. The results of this will inform future steps in the development and application of the technique.

The scope of this study has been purposely constrained to consideration of safety associated with implementing the defined AP scheme. It is recommended that additional investigation and analysis of a possible AP scheme is performed by ENW in areas such as business and operational risk, cost, legal implications and business strategy to contribute to the business case.

Subject to these additional steps, it is recommend that ENW takes forward the development of the AP scheme with appropriate level of validation of achievement of the required SIL for the solutions adopted. As part of this it would be specifically required to establish that the short term (approx. 400ms) current rating of circuit breakers and busbars is higher than current published 3 second ratings.

BIBLIOGRAPHY

- BSI Standards Publication. (2010). BS EN 61508:2010 - Functional safety of electrical/electronic/programmable electronic safety-related systems, from the BSI.
- Electricity North West. (2017). Respond technology, from ENWI: <http://www.enwl.co.uk/respond/what-we-have-learned/respond-technology>
- Energy Networks Association (ENA). (2016). SHE Standard 07, Model Distribution Safety Rules, from ENA: [http://www.energynetworks.org/assets/files/electricity/she/ENA SHE Standard 07 - Model Distribution Safety Rules \(2016\).pdf](http://www.energynetworks.org/assets/files/electricity/she/ENA_SHE_Standard_07_-_Model_Distribution_Safety_Rules_(2016).pdf)
- Health and Safety Executive. (1989). The Electricity at Work Regulations 1989, from Health and Safety Executive: <http://www.hse.gov.uk/pUbns/priced/hsr25.pdf>
- Health and Safety Executive. (2001). Reducing Risks, Protecting People, from HSE books: <http://www.hse.gov.uk/risk/theory/r2p2.pdf>
- Health and Safety Executive. (2006). The Electricity Safety, Quality and Continuity (Amendment) Regulations 2006 No. 1521, from the Construction Information Service
- Health and Safety Executive. (2009). The Electricity Safety, Quality and Continuity (Amendment) Regulations 2009 No. 639, from the Construction Information Service.
- Health and Safety Executive. (2015). Electricity at Work Regulations – Guidance on the Regulations 3rd edition, from Health and Safety Executive: <http://www.hse.gov.uk/pUbns/priced/hsr25.pdf>
- Health and Safety Executive. (2013). Electricity at work – Safe working practices 3rd edition, from Health and Safety Executive: <http://www.hse.gov.uk/pUbns/priced/hsg85.pdf>
- McTaggart, C., Cardenas, J., Lopez, A. and Bone, A. (2010). Improvements in Power System Integrity Protection Schemes. Manchester. From IET: <http://ieeexplore.ieee.org/document/5522110/>
- McTaggart, C. and Adam, D. (2016). A multilevel system integrity protection scheme based on GOOSE messaging. Edinburgh. From the IET library: <http://digital-library.theiet.org/content/conferences/10.1049/cp.2016.0074>
- National Grid. (2008). System to Generator Operational Intertripping Scheme, from National Grid UK: www2.nationalgrid.com/WorkArea/DownloadAsset.aspx?id=15308
- Scott, S., Bailey, K., Marshall, P., Turner, P. (2016). Adaptive Protection Installation and Specification Report. from ENWI: <http://www.enwl.co.uk/docs/default-source/respond-key-documents/adaptive-protection-installation-and-specification-report.pdf?sfvrsn=8>
- The Secretary of State. (2002). The Electricity Safety, Quality and Continuity Regulations 2002, from The National Archives: <http://www.legislation.gov.uk/uksi/2002/2665/contents/made>
- UK Parliament. (1974). Health and Safety at Work etc. Act 1974, from The National Archives: <http://www.legislation.gov.uk/ukpga/1974/37/contents>

APPENDIX A

HAZARD LIST

ID	HAZARD	CONSEQUENCE
1	Transformer high current caused by short circuit fault in the downstream system, i.e. on a feeder circuit.	Inconsequential. Transformers are rated on x 3 fault current.
2	Increased fault current flowing through the transformer causes increased oil degradation.	Inconsequential. Operation within rating and for a short time, causing insignificant change to the existing (non-AP) situation with regards oil degradation and ageing.
3	Transformer CB high current caused by short circuit fault in the downstream system, i.e. on a feeder circuit.	Inconsequential. Higher fault level currents than usual but within rating. Operation within rating causing insignificant change to the existing situation.
4	Increased fault current flowing through the transformer CB may cause additional degradation.	Inconsequential. Operation within rating causing insignificant change to the existing situation.
5	Bus coupler high current caused by short circuit fault in the downstream system, i.e. on a feeder circuit.	Inconsequential. Operation within rating causing insignificant change to the existing situation.
6	Increased fault current flowing through the bus coupler CB may cause additional degradation.	Inconsequential. Operation within rating causing insignificant change to the existing situation.
7	Busbar A/B high current caused by short circuit fault at the busbar.	The busbar will see a peak current and thermal impact. The peak asymmetrical fault current may be in excess of the busbar through fault current withstand rating. Excessive thermal conditions or excessive forces leading to explosion (substation structural damage) and potential fatality (workers and public).
8	Short circuit causing fault level currents in substation equipment in excess of ratings.	Explosion that could cause damage to structures and consequential potential fatality (workers and public).
9	Feeder cables high current caused by short circuit fault.	Increased fault level current could cause cable thermal rating to be exceeded (I^2t), excessive current, cable damage, cable joint explosion, substation structural damage and potential fatality (workers and public). Potentially involving interruption of adjacent utilities.
10	Feeder CB high current caused by short circuit fault at the CB.	CB required to operate beyond its rating and may not be able to interrupt the fault current. Excessive thermal conditions or excessive forces could lead to fire and explosion with potential fatality (workers and public).
11	Failure of CTs connected to the feeder CB relay.	Feeder CB will not trip when a fault current occurs, CB through fault rating may be exceeded, could lead to fire and explosion with potential fatality (workers and public).
12	Feeder CB oil degradation and increased contact wear caused by operation at higher fault levels.	Degraded operation is more likely, as is failure on demand.
13	Feeder CB oil degradation and increased contact wear caused by insufficient maintenance.	Degraded operation is more likely, as is failure on demand.
14	AP protection fault caused by loss of supply voltage or loss of CTs input (relay monitoring).	Public and workers potentially exposed to hazards due to fire or explosion resulting from any separate fault current conditions occurring between AP protection failure and control engineer action to mitigate it.

ID	HAZARD	CONSEQUENCE
15	AP relay protection loss of communication to detect AP relay health.	Public and workers potentially exposed to hazards due to fire or explosion resulting from any separate fault current conditions occurring between AP protection loss and control engineer action to mitigate it in response to 'loss of AP health' warning.
16	AP relay protection failure due to loss of supply on substation / no battery backup.	Public and workers potentially exposed to hazards due to fire or explosion resulting from any separate fault current conditions occurring between AP protection loss and control engineer action to mitigate it in response to 'loss of AP health' warning.
17	Bus coupler CB (or ring section CB) does not open when required (by AP) due to sticking or loss of control supply.	No consequence for overall AP operation. AP stage 1 HV and LV transformer CBs provide first stage of adaptive protection to reduce fault level.
18	Transformer incomer CB does not open when required due to sticking or loss of control supply.	No consequence for overall AP operation. AP stage 1 second CB trip and AP stage 2 CB trip provide backup of adaptive protection to reduce fault level.
19	AP not operational when required due to incorrect or inappropriate AP relay settings.	Reduced or zero level of AP. Public and workers potentially exposed to hazards due to fire or explosion resulting from any separate fault current conditions occurring.
20	AP not operational when required due to faulty or damaged CTs.	Reduced or zero level of AP. Public and workers potentially exposed to hazards due to fire or explosion resulting from any separate fault current conditions occurring.
21	Customer switchgear high current due to short circuit fault.	Switchgear required to operate with excessive current and/or excessive thermal conditions, could lead to fire and explosion with potential fatality (workers and public).
22	Distribution switchgear high current due to short circuit fault.	Switchgear required to operate with excessive current and/or excessive thermal conditions, could lead to fire and explosion with potential fatality (workers and public).
23	Overhead lines (OHL) high current due to short circuit fault.	Could cause cable thermal rating to be exceeded (I^2t) Increased fault level current could cause cable thermal rating to be exceeded (I^2t), excessive current, cable damage, cable clearance limits being exceeded, substation structural damage and potential fatality (workers and public).

APPENDIX B EVENT TREES

Short circuit of the busbar in a substation resulting in excessive fault current

Busbar A/B high current due to short circuit fault.	AP operation	Workforce comply with exclusion procedure for operating substation. Workforce not in fatality risk zone at time of hazard occurrence.	Public not in fatality risk zone at time of hazard occurrence. (Figure is for High Risk)	All consequences (per site)	Frequency (per annum across ENW) 1001	Frequency (per annum across ENW) 1002
λ (frequency per annum per site)	N (detected fault)	N	N	1.42E-02		
0.01423669	3.45205E-05	0.00001	0			
			Y			
			1	Workforce fatality. Severe asset damage.	1.39E-09	9.74E-09
		Y	N			
		0.99999	0.1	Public fatality. Severe asset damage.	1.39E-05	4.17E-05
			A			
			0.9	Severe asset damage.	1.25E-04	9.73E-05
	N (undetected fault)	N	N			
	0.0042	0.00001	0			
			Y			
			1	Workforce fatality Severe asset damage.	1.69E-07	9.17E-09
		Y	N			
		0.99999	0.1	Public fatality. Severe asset damage.	1.69E-03	9.17E-05
			Y			
			0.9	Severe asset damage.	1.52E-02	8.25E-04
	Y					
	0.995765479			Asset fault. Service limitation. Maintenance activity.	4.01E+00	4.01E+00

Short circuit of the feeder cables or something connected to these cables such that the feeder cable withstand current is exceeded

Feeder cables high current with AP operation cable thermal rating exceedance (I ² t) due to short circuit fault.	Workforce comply with exclusion procedure for operating substation. Workforce not in fatality risk zone at time of hazard occurrence.	Public not in fatality risk zone at time of hazard occurrence.	All consequences (per site)	Frequency (per annum across ENW) 1001	Frequency (per annum across ENW) 1002
λ (frequency per annum per site)	N (detected fault)	N	N	3.22E-01	
0.322	3.45205E-05	0.00001	0		
			Y		
			1	3.15E-08	1.56814E-07
			Workforce fatality. Severe asset damage.		
		Y	N		
		0.99999	0.1	3.15E-04	4.71811E-06
			Y		
			0.9	2.83E-03	0.001567984
			Severe asset damage.		
	N (undetected fault)	N	N		
	0.0042	0.00001	0		
			Y		
			1	3.83E-06	2.07E-07
			Workforce fatality. Severe asset damage.		
		Y	N		
		0.99999	0.1	3.83E-02	2.07E-03
			Y		
			0.9	3.44E-01	1.87E-02
			Severe asset damage.		
	Y			9.07E+01	45.37006254
	0.995765479				
			Asset fault. Service limitation. Maintenance activity.		

Short circuit within a Circuit Breaker in the substation resulting in excessive fault current

Feeder CBs high current due to short circuit fault.	AP operation	Workforce comply with exclusion procedure for operating substation. Workforce not in fatality risk zone at time of hazard occurrence.	Public not in fatality risk zone at time of hazard occurrence.	All consequences (per site)	Frequency (per annum across ENW) 1001	Frequency (per annum across ENW) 1002
λ (frequency per annum per site)	N (detected fault)	N	N			
0.0022	3.45205E-05	0.00001	0			
			Y			
			1	Workforce fatality. Severe asset damage.	2.15E-10	1.87535E-09
		Y	N			
		0.99999	0.1	Public fatality. Severe asset damage.	2.15E-06	2.73873E-06
			Y			
			0.9	Severe asset damage.	1.93E-05	1.87516E-05
	N (undetected fault)	N	N			
	0.0042	0.00001	0			
			Y			
			1	Workforce fatality. Severe asset damage.	2.61E-08	1.42E-09
		Y	N			
		0.99999	0.1	Public fatality. Severe asset damage.	2.61E-04	1.42E-05
			Y			
			0.9	Severe asset damage.	2.35E-03	1.28E-04
	Y					
	0.995765479			Asset fault. Service limitation. Maintenance activity.	6.20E-01	0.619963588

Short circuit of the Overhead Line or something connected to the Overhead Line such that the Overhead Line withstand current is exceeded

Overhead lines (OHL) high current with cable thermal rating exceedance (I^2t) due to short circuit fault.	AP operation	Workforce comply with exclusion procedure for operating substation. Workforce not in fatality risk zone at time of hazard occurrence.	Public not in fatality risk zone at time of hazard occurrence.	All consequences (per site)	Frequency (per annum across ENW) 1001	Frequency (per annum across ENW) 1002	
λ (frequency per annum per site)	N (detected fault)	N	N				
0.4284	3.45205E-05	0.00001	0				
			Y	1	Workforce fatality. Severe asset damage.	4.19E-08	3.47718E-07
		Y	N	0.1	Public fatality. Severe asset damage.	4.19E-04	1.04619E-05
		0.99999	Y	0.9	Severe asset damage.	3.77E-03	0.003476835
	N (undetected fault)	N	N				
	0.0042	0.00001	0				
			Y	1	Workforce fatality. Severe asset damage.	5.09E-06	2.76E-07
		Y	N	0.1	Public fatality. Severe asset damage.	5.09E-02	2.76E-03
		0.99999	Y	0.9	Severe asset damage.	4.58E-01	2.48E-02
	Y				Asset fault. Service limitation. Maintenance activity.	1.21E+02	100.6031822
	0.995765479						

APPENDIX C

SAFETY REQUIREMENTS

ID.	RELATED HAZARDS	DESCRIPTION
SR1	7, 8, 9, 10, 11, 23	Apply adaptive protection
SR2	7, 9, 10, 11, 23	Overcurrent protection - Tx HV side (where required)
SR3	7, 9, 10, 11, 23	Busbar able to withstand peak instantaneous fault current if AP is installed and working up until stage 2 of AP protection has operated
SR4	7, 9, 10, 11, 23	Busbar able to withstand the prospective thermal (I^2t) impact if AP is installed and working up until stage 2 of AP protection has operated
SR5	7, 9, 10, 11, 23	Before workforce enter substation, ensure operational procedures are followed to reduce prospective fault current to within limits (open busbar CB)
SR6	7, 9, 10, 11, 23	AP target failure measure Safety Integrity Level (SIL) as determined by risk assessment
SR7	7, 8, 9, 10, 11, 23	Substation structure explosion withstand capability; blast wall, additional containment, pressure relief (For high risk sites)
SR8		9 Feeder cables able to withstand maximum fault current if AP is installed and working up until stage 2 of AP protection has operated
SR9		9 Feeder cables able to withstand the thermal impact due to the flow of the maximum prospective fault current if AP is installed and working up until stage 2 of AP protection has operated
SR10	12, 13	Maintenance of CBs, Txs and busbars should appropriately reflect the frequency of operation
SR11	9, 10, 11, 23	Feeder CB able to withstand the peak making current if AP is installed and working up until stage 2 of AP protection has operated
SR12	9, 10, 11, 23	Feeder CB able to withstand the prospective thermal (I^2t) impact if AP is installed and working up until stage 2 of AP protection has operated
SR13	14	AP only to be applied where there is an alarm/warning system in the Control Room to indicate an AP relay issue/problem

ID.	RELATED HAZARDS	DESCRIPTION
SR14	14, 15	Control engineer manually issues a signal to open the bus section to mitigate the fault level issue, in response to AP relay alarm
SR15	16	Alarm/warning system in the Control Room to indicate substation power supply fault/loss.
SR16	16	Control engineer manually issues a signal to operate upstream protection, in response to 'substation power supply fault/loss' alarm
SR17	16	AP should only be applied where the fault level can be brought within rating by switching upstream.
SR18	17, 18	Provision of second stage trip by AP
SR19	19	Planning to specify appropriate settings for AP which are revised when any connections are added to the network to ensure that the switchgear is adequately rated, revised when the fault level changes, revised if the network is reconfigured or altered in a way that would change the prospective fault current at any location within the network
SR20	19	Satisfactory commissioning of AP protection relays
SR21	20	AP to be implemented with a single phase setting well above the prospective single phase fault current so that it doesn't respond to the failure of one CT
SR22	20	AP to be implemented with a minimum current setting warning/alarm that will indicate a problem with one of the CTs showing a very low current
SR23	21	AP only to be applied where the prospective fault current is within the rating of existing customer switchgear on any feeder or the fault level at a customers' site is equal to or less than the design fault level even if AP fails to operate
SR24	22	AP only to be applied where the prospective fault current is within the rating of existing distribution switchgear on any feeder if AP is installed and working up until stage 2 of AP protection has operated
SR25	23	AP only to be applied where the prospective fault current is within the thermal capacity of any overhead lines if AP is installed and working up until stage 2 of AP protection has operated
SR26	17	Periodic proof testing of AP system and equipment to confirm all components functioning as intended and free of faults.
SR27	1,2,3,4	Transformer fault currents are within the rating of the transformer and its circuit breaker even if AP protection fails
SR28	5,6	Bus coupler fault currents are within the rating of its circuit breaker even if AP protection fails

APPENDIX D

KEY REQUIREMENTS OF HEALTH & SAFETY APPLICABLE LEGISLATION

Note: The table below is not a complete definition of requirements from legislation applying to the design, implementation of an AP scheme. It presents extracts from some relevant legislation and supplemental guidance – refer to original Acts, Regulations and associated supplemental guidance publications for a full description of requirements.

LEGISLATION AND GUIDANCE REFERENCE DESCRIPTION

LEGISLATION AND GUIDANCE	REFERENCE	DESCRIPTION
HSW Act	Part 1, Section 2 (1)	General duties of employers to their employees: It shall be the duty of every employer to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all his employees.
	Part 1, Section 2 (2)	General duties of employers to their employees: (a) the provision and maintenance of plant and systems of work that are, so far as is reasonably practicable, safe and without risks to health; (b) arrangements for ensuring, so far as is reasonably practicable, safety and absence of risks to health in connection with the use, handling, storage and transport of articles and substances; (c) the provision of such information, instruction, training and supervision as is necessary to ensure, so far as is reasonably practicable, the health and safety at work of his employees; (d) so far as is reasonably practicable as regards any place of work under the employer's control, the maintenance of it in a condition that is safe and without risks to health and the provision and maintenance of means of access to and egress from it that are safe and without such risks; (e) the provision and maintenance of a working environment for his employees that is, so far as is reasonably practicable, safe, without risks to health, and adequate as regards facilities and arrangements for their welfare at work.
	Part 1, Section 3 (1)	General duties of employers and self-employed to persons other than their employees: It shall be the duty of every employer to conduct his undertaking in such a way as to ensure, so far as is reasonably practicable, that persons not in his employment who may be affected thereby are not thereby exposed to risks to their health or safety.
	Part 1, Section 6 (1)	General duties of manufacturers etc. as regards articles and substances for use at work. It shall be the duty of any person who designs, manufactures, imports or supplies any article for use at work- (a) to ensure, so far as is reasonably practicable, that the article is so designed and constructed that it will be safe and without risks to health at all times when it is being set, used, cleaned or maintained by a person at work; (b) to carry out or arrange for the carrying out of such testing and examination as may be necessary for the performance of the duty imposed on him by the preceding paragraph.

LEGISLATION AND GUIDANCE REFERENCE DESCRIPTION

	Part 1, Section 6 (2)	It shall be the duty of any person who undertakes the design or manufacture of any article for use at work to carry out or arrange for the carrying out of any necessary research with a view to the discovery and, so far as is reasonably practicable, the elimination or minimisation of any risks to health or safety to which the design or article may give rise.
Management of HSW Regulations	Regulation 3, (1)	Risk assessment: Every employer shall make a suitable and sufficient assessment of: a) The risks to the health and safety of his employees to which they are exposed whilst they are at work; and b) The risks to the health and safety of persons not in his employment arising out of or in connection with the conduct by him of his undertaking.
EAW Regulations	Regulation 4, (1)	All systems shall at all times be of such construction as to prevent, so far as is reasonably practicable, danger.
	Regulation 5	No electrical equipment shall be put into use where its strength and capability may be exceeded in such a way as may give rise to danger.
	Regulation 6	Electrical equipment which may reasonably foreseeably be exposed to: (a) mechanical damage; (b) the effects of the weather, natural hazards, temperature or pressure; (c) the effects of wet, dirty, dusty or corrosive conditions; or (d) any flammable or explosive substance, including dusts, vapours or gases, shall be of such construction or as necessary protected as to prevent, so far as is reasonably practicable, danger arising from such exposure.
	Regulation 11	Efficient means, suitably located, shall be provided for protecting from excess of current every part of a system as may be necessary to prevent danger.
	Regulation 12, (1)	Where necessary to prevent danger, suitable means (including, where appropriate, methods of identifying circuits) shall be available for—: (a) cutting off the supply of electrical energy to any electrical equipment; and (b) the isolation of any electrical equipment.
	Regulation 29	In any proceedings for an offence consisting of a contravention of regulations 4(4), 5, 8, 9, 10, 11, 12, 13, 14, 15, 16 or 25, it shall be a defence for any person to prove that he took all reasonable steps and exercised all due diligence to avoid the commission of that offence.
HSR25 2015	<i>Absolute/ Reasonably Practicable</i>	
	...Clause 57	Duties in some of the Regulations are subject to the qualifying term 'reasonably practicable'. Where qualifying terms are absent the requirement in the regulation is said to be absolute. The meaning of reasonably practicable has been well established in law. The interpretations in paragraphs 59–60 are given only as a guide to dutyholders.
	...Clause 58	If the requirement in a regulation is 'absolute', for example if the requirement is not qualified by the words 'so far as is reasonably practicable', the requirement must be met regardless of cost or any other consideration. Regulations making such absolute requirements are subject to the defence provision of regulation 29.
	<i>Regulation 5</i> ...	
	...Clause 80	The defence (regulation 29) is available in any proceedings for an offence under this regulation.

LEGISLATION AND GUIDANCE REFERENCE DESCRIPTION

	Clause 81	Before equipment is energised, the characteristics of the system to which the equipment is connected must be taken into account. This should include those existing under normal conditions, possible transient conditions and prospective fault conditions, so that the equipment is not subjected to stress which it is not capable of handling without giving rise to danger. The effects to be considered include voltage stress and the heating and electromagnetic effects of current.
	Clause 82	The term 'strength and capability' of electrical equipment refers to the ability of the equipment to withstand the thermal, electromagnetic, electrochemical or other effects of the electrical currents which might be expected to flow when the equipment is part of a system. These currents include, for example, load currents, transient overloads, fault currents, pulses of current and, for alternating current circuits, currents at various power factors and frequencies. Insulation must be effective to enable the equipment to withstand the applied voltage and any likely transient over-voltages.
	Clause 83	A knowledge of the electrical specification and the tests, usually based on the requirements of national or international standards, will assist the user in identifying the withstand properties of the equipment so that it may be selected and installed to comply with this regulation. Such tests are normally carried out either by the manufacturer or by an accredited testing organisation.
	Clause 84	The strength and capability of electrical equipment is not necessarily the same as its rating. Usually the rating is that which has been assigned by the manufacturer following a number of agreed tests.
	Clause 85	Electrical equipment should be used within the manufacturer's rating (continuous, intermittent or fault rating as appropriate) and in accordance with any instructions supplied with the equipment.
	Clause 86	So that equipment remains safe under prospective fault conditions, you must select equipment that takes account of the fault levels and the characteristics of the electrical protection which has been provided for the purpose of interrupting or reducing fault current (excess current protection is required by regulation 11). Most electrical equipment will be able to withstand short-circuit currents safely for limited periods only. The considerations also extend to conductors and equipment provided solely for protective purposes, eg earthing conductors must be adequately rated to survive beyond fault clearance times to ensure satisfactory protective gear operation and fault clearance.
	<i>Regulation ... 11</i>	
	...Clause 167	The defence (regulation 29) is available in any proceedings for an offence under this regulation (see paragraphs 177–179).
	Clause 168	It is recognised that faults and overloads may occur on electrical systems. The regulation requires that systems and parts of systems be protected against the effects of short circuits and overloads if these would result in currents which would otherwise result in danger.
	Clause 169	The means of protection is likely to be in the form of fuses or circuit breakers controlled by relays etc, or it may be provided by some other means capable of interrupting the current or reducing it to a safe value.
	Clause 172	When selecting the means of protection, you must consider a number of factors – the more important of these include: (a) the nature of the circuits and type of equipment to be protected; (b) the short-circuit energy available in the supply (the fault level); (c) the nature of the environment; (d) whether the system is earthed or not.

LEGISLATION AND GUIDANCE REFERENCE DESCRIPTION

	Clause 173	The circuits to be dealt with may vary from high-power, high-voltage circuits, eg for the inter-connection of substations or for the supply to large motors, down to the smallest final circuit supplying a few low-power lamps at, say, 6 V. Over this range lies a great diversity of equipment, each item of which will possess characteristics which must be carefully considered in the selection of appropriate devices to protect against excess current.
	Clause 174	The maximum short-circuit current in the protected circuit must be considered. (The ability of circuit breakers and fuses to operate successfully and without dangerous effects, serious arcing or, in the case of oil-filled equipment, the liberation of oil, is implicit in the requirements of regulations 4 and 5.) The design of the protective arrangement must also provide for sufficient current to be available to operate the protective devices correctly in respect of all likely faults.
	Clause 177	The defence (regulation 29) is available in any proceedings for an offence under this regulation.
	Clause 178	In some circumstances it will be technically impossible to achieve total compliance with the absolute requirement to prevent danger. If an excess of current is drawn due to a fault or overload, eg due to an arcing fault, then whatever form of electrical protection is provided, there will be some danger at the point of the fault during the finite time taken for the detection and interruption of the fault current. Nevertheless, electrical protection – whether by means of a simple fuse or another method – must be properly chosen and installed in accordance with good electrical engineering practice. The protection must be efficient and effective.
	<i>Regulation ... 12</i>	
	...Clause 185	The need for means to cut off the supply and effect isolation depends on factors such as likely danger in normal and abnormal conditions. This assessment may be influenced by environmental conditions and provisions to be made in case of emergencies, such as a fire in premises. It includes consideration of which electrical equipment could be a source of danger if such means were not provided and of the installation, commissioning, operational and maintenance requirements over the life of the equipment.
	<i>Regulation ... 29</i>	
	...Clause 244	Regulation 29 applies only in criminal proceedings. It provides a defence for a dutyholder who can establish that they took all reasonable steps and exercised all due diligence to avoid committing an offence under regulations 4(4), 5, 8, 9, 10, 11, 12, 13, 14, 15 or 16.
HSG85 2013	Clause 8	Equipment must be properly designed, constructed, installed and maintained so that it does not present a risk of electric shock, burns, fire or explosion when properly used.
	Clause 12	You must select equipment that is suitable for the environment in which it is used, for example cables and equipment in heavy industries such as sheet metal works need to be protected against mechanical damage. You should consider adverse environmental factors when working on equipment. For example, excessively damp or humid conditions will increase the risk of injury because of reduced effectiveness of insulation, which may undermine the effectiveness of devices used for isolation, or increase the severity should an electric shock occur. Equipment that has corroded may not function as intended.

LEGISLATION AND GUIDANCE **REFERENCE DESCRIPTION**

LEGISLATION AND GUIDANCE	REFERENCE	DESCRIPTION
ESQC Regulations	Regulation 3, (1)	Generators, distributors and meter operators shall ensure that their equipment is: (a) sufficient for the purposes for and the circumstances in which it is used; and (b) so constructed, installed, protected (both electrically and mechanically), used and maintained as to prevent danger, interference with or interruption of supply, so far as is reasonably practicable.
	Regulation 4	Generators, distributors, suppliers and meter operators shall: (a) disclose such information to each other as might reasonably be required in order to ensure compliance with these Regulations; and (b) otherwise co-operate amongst themselves so far as is necessary in order to ensure compliance with these Regulations.
	Regulation 6	A generator or distributor shall be responsible for the application of such protective devices to his network as will, so far as is reasonably practicable, prevent any current, including any leakage to earth, from flowing in any part of his network for such a period that that part of his network can no longer carry that current without danger.
	Regulation 23, (1)	A distributor shall ensure that his network shall be: (a) so arranged; and (b) so provided, where necessary, with fuses or automatic switching devices, appropriately located and set, as to restrict, so far as is reasonably practicable, the number of consumers affected by any fault in his network.
	Regulation 24, (1)	A distributor or meter operator shall ensure that each item of his equipment which is on a consumer's premises but which is not under the control of the consumer (whether forming part of the consumer's installation or not) is: (a) suitable for its purpose; (b) installed and, so far as is reasonably practicable, maintained so as to prevent danger; and (c) protected by a suitable fusible cut-out or circuit breaker which is situated as close as is reasonably practicable to the supply terminals.
	Regulation 28	A distributor shall provide, in respect of any existing or proposed consumer's installation which is connected or is to be connected to his network, to any person who can show a reasonable cause for requiring the information, a written statement of— (a) the maximum prospective short circuit current at the supply terminals; (b) for low voltage connections, the maximum earth loop impedance of the earth fault path outside the installation; (c) the type and rating of the distributor's protective device or devices nearest to the supply terminals; (d) the type of earthing system applicable to the connection; and (e) the information specified in regulation 27(1), which apply, or will apply, to that installation.