Powerful-CB

Safety Case Process and Principles

FNC 52680/45804R Issue 1

Prepared for UK Power Networks

SYSTEMS AND ENGINEERING TECHNOLOGY

DOCUMENT INFORMATION

Project : Powerful-CB

Report Title : Safety Case Process and Principles

Client : UK Power Networks

Client Ref. : 7600003478

Classification :

Report No. : FNC 52680/45804R

Issue No. : 1

Date : 5th May 2017

Compiled By : John Stringer

Verified By : Richard Wheldon

Approved By : Richard Wheldon

Signed : *Original signed*

DISTRIBUTION

Copy	Recipient	Organisation
1	Li-Wen Yip	UK Power Networks
2	File	Frazer-Nash Consultancy

Copy No.: _____

Originating Office: FRAZER-NASH CONSULTANCY LIMITED
Stonebridge House, Dorking Business Park, Dorking, Surrey, RH4 1HJ
T: 01306 885050 F: 01306 886464 W: www.fnc.co.uk

ACRONYMS AND ABBREVIATIONS

ALARP	As Low As Reasonably Practicable
AMAT	Applied Materials
BAU	Business As Usual
CAE	Claims, Arguments and Evidence
CoP	Code of Practice
CSM REA	Common Safety Method for Risk Evaluation and Assessment
DNO	Distribution Network Operator
ENA	Energy Networks Association
FLCB	Fault Limiting Circuit Breakers
FMEA	Failure Mode and Effects Analysis
HAZID	Hazard Identification
I	Incident
NIC	Network Innovation Competition
R2P2	Reducing Risks, Protecting People
RACI	Responsible, Accountable, Consulted, Informed
RIDDOR	Reporting of Injuries, Diseases and Dangerous Occurrence
PSC	Preliminary Safety Case
PSCR	Preliminary Safety Case Report
SI	Serious Incident
TOR	Tolerability of Risk
UKPN	UK Power Networks
VSI	Very Serious Incident

GLOSSARY OF TERMS

For consistency and ease of reference the following terminology is defined below:

Accident	An unintended event, or sequence of events, that causes harm.
ALARP	A risk is ALARP when it has been demonstrated that the cost of any further risk reduction is grossly disproportionate to the safety benefit obtained from that risk reduction.
Claim	An assertion that contributes to the safety argument.
Consequence	The outcome, or outcomes, resulting from an event.
Evidence	Records, statements, facts or other information, which are relevant to the audit criteria and verifiable.
Harm	Death, physical injury or damage to the health of people.
Hazard	A physical situation or state of a system, often following from some initiating event, that may lead to an accident. Anything presenting the 'possibility of danger' is also regarded as a 'hazard'.
Hazard Identification	The process of identifying and listing the hazards and accident sequence associated with a system.
Lost Time Incident	Where any person at work is incapacitated for routine work for more than one day (excluding the day of the accident) because of an injury resulting from an accident arising out of or in connection with that work. If this period exceed seven consecutive days then this is reportable under RIDDOR.
Medical Treatment Injury	Work-related injury resulting in treatment from a professional medical person e.g. nurse or a doctor in a hospital, from their own GP or paramedic etc. but does not result in a Lost Time Incident.
Personal Injury	A work-related injury of a minor nature and where the injured person receives.
Risk	Combination of the likelihood of harm and the severity of that harm.
Risk Reduction	The systematic process of reducing risk.
Safety Case	A structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment.
Safety Case Report	A report that summarises the arguments and evidence of the Safety Case at a given point in time.
Tolerability Limits	The boundaries of individual risk, between which the level of risk may be tolerated when it has been demonstrated that the risk is ALARP and is not unacceptable. Different individual risk limits are set for workers and the general public.

CONTENTS

1. INTRODUCTION

1.1 BACKGROUND

Fault Limiting Circuit Breakers (FLCBs) provide a means to allow the continued growth and connection of distributed generation onto the National Grid in a cost-effective manner. To allow use of FLCBs, the safety risks of using this novel, power electronics based technology must be understood, managed and shown to be Tolerable and As Low As Reasonably Practicable (ALARP).

These devices have only been developed to proof of concept stage and are currently not used anywhere in the world. UK Power Networks (UKPN) have secured funding for a dual trial of two different, innovative, FLCBs on 11kV networks through the Ofgem introduced Electricity Network Innovation Competition (NIC):

- The first device, produced by ABB, is designed for deployment in network substations.
- The second, produced by Applied Materials (AMAT), is designed for customer connection points.

Parallel trials will provide insight to stakeholders on the relative suitability of each technology in two different configurations, as well as data on the performance of each solution. A successful outcome of the trials will accelerate the development and adoption of these devices. The desired successful outcome of the trials is, however, dependent on FLCBs being shown to be safe. For example, if the FLCB fails to operate on demand in a BAU (Business As Usual) installation, the downstream network could be exposed to a fault current exceeding its rating. In extreme circumstances, this could result in a failure of the downstream equipment which may harm people.

1.2 SAFETY CASE REQUIREMENT

A Safety Case is required in order to support the development of the two FLCB devices and to demonstrate that their use on an 11kV electrical network is tolerably safe. The Safety Case should also demonstrate that the safety management system (i.e. policy, organisation, documentation, training, performance monitoring, change control etc.) is adequate to ensure compliance with the relevant safety legislation, including:

- The Health and Safety at Work etc. Act 1974 [1];
- The Management of Health and Safety at Work Regulations 1999 [2];
- The Electricity at Work Regulations 1989 [3], particularly regulations 4.1/5/11;
- The Electricity Safety, Quality and Continuity Regulations 2002 [4], particularly regulations 3.1/6.

Initially, this will be limited to supporting the two trials, but will be developed further in future iterations to include functional testing and commissioning, extended operation testing, and ultimately its general use / roll out on the network.

Development of these safety cases is based upon a feasibility study carried out by Frazer-Nash Consultancy (Frazer-Nash) in 2016 [5].

1.3 DOCUMENT PURPOSE

The purpose of this document is to define the process for production, review and approval of the safety case for each device, define the safety case principles, and communicate the approach to safety to all relevant affected project stakeholders.

2. SCOPE OF THE SAFETY CASE

The scope of the Safety Case will be bound by the two FLCB devices themselves, their functionality and the environment they will operate in. Initially, this will be constrained to the two trials but will also need to consider BAU operation on the wider 11kV network (i.e. a generic application case) in order to ensure that the Safety Case is comprehensive. This will be developed as part of the Safety Management process (see Section 3).

The Safety Case itself will identify and demonstrate compliance with the following:

- Legislative and regulatory requirements e.g. Electricity at Work Regulations.
- UKPN safety procedures, guidance and design standards e.g. Distribution Safety Rules, safe systems of work, operational procedures etc.
- Safety Requirements derived from national and International standards e.g. EN 50160, IEC TR 62063:1999, and relevant parts of IEC 62271 etc.
- Safety Requirements derived from the hazard identification (HAZID) and risk assessment process.

It is recognised that compliance with the Electricity at Work Regulations is essential in order to demonstrate safe operation. However, it is important to consider Regulation 5, which states '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.' The key aspect of this requirement is the mandate that equipment must not fail or fail to operate in such a way that may give rise to danger. This does not prescriptively prevent the use of a FLCB to increase the level of potential fault current; however, it requires that:

"Each FL-CB device and the corresponding protection measures shall be sufficiently reliable, or have suitable mitigation installed, such that the likelihood of the network equipment seeing a fault current above its rating is 'Broadly Acceptably' or that the risk has been reduced to be 'Tolerable' and ALARP."

Ultimately the Safety Case will need to demonstrate that the devices and their use in both trials and general application will be considered to be 'Safe' i.e. when the risks have been demonstrated to have been reduced to a level that is 'Broadly Acceptable', or 'Tolerable' and ALARP, and relevant prescriptive Safety Requirements have been met. Adherence to the safety case principles derived herein (see Section 6.1) will be used to determine whether a suitable 'case for safety' has been made.

3. SAFETY MANAGEMENT PROCESS

3.1 OVERVIEW

This section describes the safety management process and how it will be used to produce the safety case for the two devices. An overview of the process is shown in Figure 1.

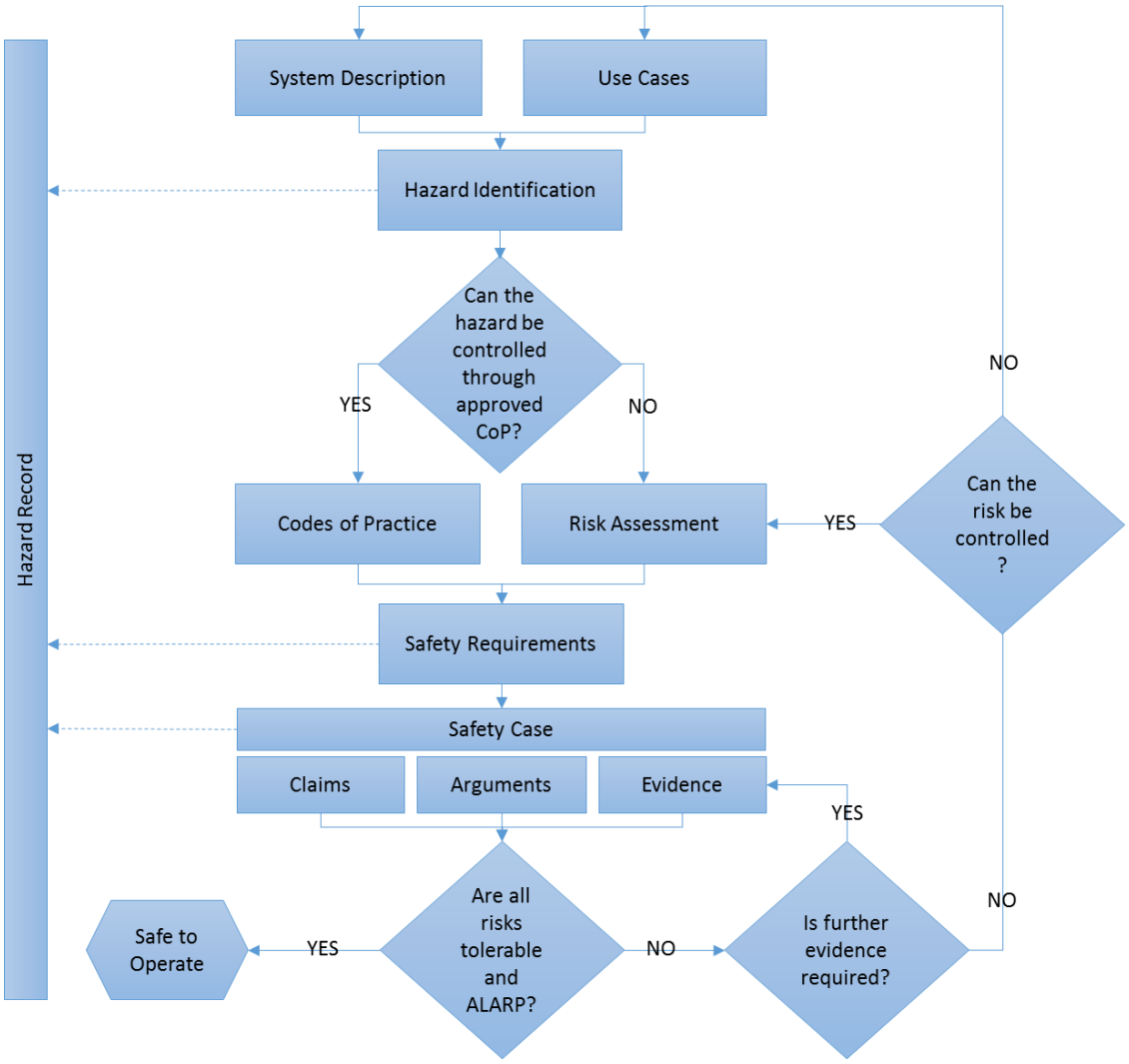

Figure 1: Safety Management Process

3.2 DEFINE SYSTEM DESCRIPTION / USE CASES

In order to bound the scope of the Safety Case it is important to explicitly define and describe the two devices and their use cases. This will ensure that the subsequent Hazard Identification (HAZID) and analysis activities are well focussed and provide credible evidence to the safety case process. The system description / use cases should as a minimum address the system boundary, operating environment, physical and functional interfaces plus any assumptions that determine the limits for the risk assessment. The system description / use cases will form part of the briefing pack for the HAZID workshop (see Section 3.3).

Presently, the following use cases may be considered, where appropriate, to the device in question, although they will need to be further developed:

- ABB Device - FLCB installed at a Distribution Network Operator (DNO) 11kV substation, in series with a transformer incomer or interconnector or in parallel with a bus coupler/tie, to enable the prospective fault level to be increased beyond the rating of the substation or downstream equipment.
- AMAT Device - FLCB installed at a customer's premises in series with a generator, to reduce or eliminate the generator's contribution to the network fault level.

3.3 HAZARD IDENTIFICATION

The purpose of the HAZID is to identify all reasonably foreseeable hazards which are then assessed. The HAZID should be systematic and structured. Correct HAZID will underpin the whole risk management process and give assurance that the risks will be managed in the project. The HAZID also aims to identify all existing control measures that are in place to either prevent the occurrence of a hazardous event or to mitigate the consequences.

For the Powerful-CB project this will principally involve conducting a HAZID workshop for each device. The HAZID workshops will be preceded by a Briefing Note which will describe the system or subsystems and scope to be considered and the methodology being proposed for use in that workshop. The workshops will be chaired and staffed by Suitably Qualified and Experienced (SQEP) persons, and a record of their relevant qualifications and experience will be kept. Prior to commencement of the workshop, the team present will be assessed by the HAZID Chairman to confirm they are SQEP.

The HAZID workshops will be supplemented by a review of equipment Failure Mode and Effects Analysis (FMEA) or similar analysis conducted by each of the device manufacturers.

3.4 HAZARD RECORD

A Hazard Record will be produced for each device to capture the output from the HAZID activities above. The Hazard Record is a live document and will be continually updated throughout the project.

3.5 CODES OF PRACTICE

Some hazards may be suitably controlled through the application of UKPN policies and procedures (e.g. application of distribution safety rules) or by adherence to Regulations (e.g. compliance with Electricity at Work Regulations). Where this is identified as being the case no further risk assessment will be undertaken. The relevant policies, procedures or regulation will be recorded in the Hazard Record.

3.6 RISK ASSESSMENT

Where policies, procedures or regulations do not control the risk sufficiently, an engineering assessment will be performed to control the risks to be Tolerable and ALARP. Each hazard will be assessed to determine the exposure group, likelihood of occurrence, and consequence.

The frequency will be assessed on a quantitative basis per year of operations. These values will need to be supported by failure data other analysis (e.g. Fault Tree Analysis) from the manufacturers.

Consequence will be assessed in terms of injuries and fatalities to the different exposure groups (i.e. workers and members of the public). The definitions for personnel injury have been taken from UKPNs Incident Reporting procedure [7] derived from the Reporting of Injuries, Diseases and Dangerous Occurrence Regulations (RIDDOR) [6]. Consequences to the environment or property / plant damage will also be considered – although recognising that the risks to personnel will likely drive the consequence categorisation.

A risk matrix (see Section 6.3) will then be used to determine if the risk is low enough to be 'Broadly Acceptable' or whether further risk reduction is required to ensure risks are reduced to be 'Tolerable' and ALARP.

3.7 SAFETY REQUIREMENTS

In order to demonstrate that risk associated with the adoption of the FLCBs is reduced to be Tolerable and ALARP, control measures (i.e. design changes, additional control measures) that are applicable to the design, installation, testing and commissioning of the devices must be identified. Where relevant, control measures identified by the hazard management process will be designated as Safety Requirements. Safety Requirements will also be derived from the relevant applicable policies, procedures or regulations. Compliance against these requirements will be a key part of the evidence needed to build the safety case and therefore will form the basis of the acceptance criteria for the laboratory testing and field trials for each device.

3.8 SAFETY CASE

The safety 'Claims, Arguments and Evidence', along with the Safety Requirements will be summarised in the Safety Case which is described in detail, along with the review and approval process in Section 4.

4. SAFETY CASE, REVIEW AND APPROVAL PROCESS

4.1 SAFETY CASE DEVELOPMENT

The overall safety argument for the two devices will be expressed as 'Claims, Arguments and Evidence' (CAE). The highest level of this structure are the safety claims: these can be thought about as the high level safety 'goals' that, if all successfully achieved, result in the system or activity having a level of safety that can be considered 'Tolerable' and ALARP. Each of the claims are supported and explained by a series of arguments. Each argument must then be substantiated with a set of robust evidence. Evidence does not need to be supported by further arguments or evidence, but should contain factual information and should not involve subjective judgement.

Development of the safety case for each device will be split into 3 phases, to coincide with the development of the FLCB technology installations, as shown in Figure 2.

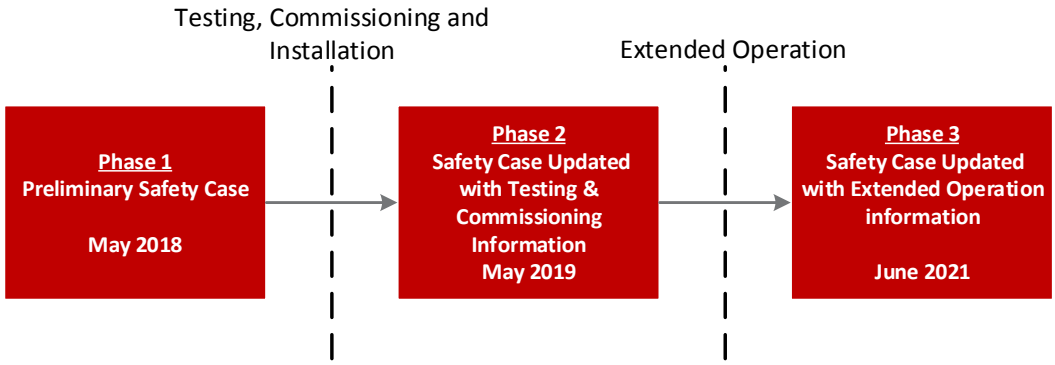

Figure 2: Safety Case Phased Development Process

4.1.1 Preliminary Safety Case Report (Phase 1)

Phase 1 is the establishment of a Preliminary Safety Case (PSC) which will form the basis for work in future phases. The claims, arguments and evidence of the PSC, along with the Safety Requirements will be summarised in a Preliminary Safety Case Report (PSCR) at the end of Phase 1. The PSCR will be subject to a review and approval process as described in Section 4.2. A separate PSCR will be produced for each of the two devices.

4.1.2 Phases 2 and 3 SCR

Phases 2 and 3 are extensions of the PSC, incorporating additional information from the further development of each of the FLCB solutions and the results from the trials carried out by UKPN. The results from the device trials, as well as design additions and modifications by ABB and AMAT, will be used to reconsider and update elements of the safety cases in Phase 2. Outputs from Phase 2 may include any additional mitigations that are required, and safety and information requirements for the extended operation testing in Phase 3.

Similarly, the results from the extended operational trials in Phase 3 will be used to update the safety cases, such that the safety of the FLCB systems can be justified for commercial operation.

4.3 REVIEW AND APPROVAL PROCESS

An overview of the process is shown in Figure 3.

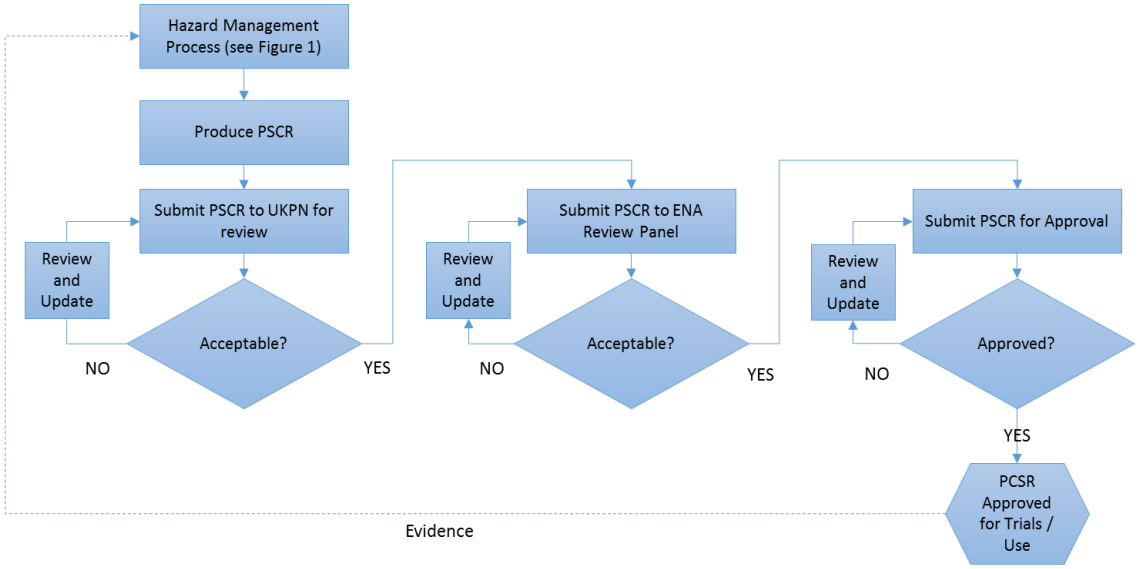

Figure 3: Safety Case Approval Process

4.3.1 UKPN Review

The PSCR will be reviewed by UKPN to provide assurance that they are content with the delivery. This will follow UKPN internal review process involving members of the UKPN project team as detailed in the safety organisation chart in Figure 4 (page 14).

4.3.2 ENA Review Panel

The PSCR will then be subject to peer review by the Energy Networks Association (ENA) Review Panel. Although not seeking approval at this stage, this panel of DNO representatives provides a level of confidence in the application of the FLCB devices, and in the robustness of the safety case.

4.3.3 Safety Case Approval

Unlike in other industries, an independent review function has not been established for the FLCB safety cases. Therefore, the UKPN Operational Safety Manager will have ultimate responsibility for approval of the safety cases and is intended to participate in the role of Design Authority during the project. In addition, the UKPN Director of Asset Management has ultimate accountability for the Powerful-CB project as a whole and therefore will also need to be consulted prior to final approval.

5. STAKEHOLDERS

5.1 RACI

A Responsible, Accountable, Consulted, Informed (RACI) matrix is a means of linking process or activity steps to roles. The tasks and associated roles within this plan have been assigned in Table 1. The persons occupying each role are shown in Figure 4 in Section 5.2. The definitions associated with this RACI matrix can be found below.

Table 1: RACI Matrix

RACI DETAILS									
• R – Responsible: the individual(s) who perform an activity – responsible for action / implementation – although usually only one, Rs can be shared. • A – Accountable: the individual who is ultimately accountable including yes/no decision and power of veto – only one 'A' can be assigned. • C – Consulted: the individual(s) to be consulted prior to a final decision being made or action taken – two-way communication. • I – Informed: the individual(s) who need to be informed after a decision is made or action is taken – one-way communication.	Project Manager (UKPN)	Safety Lead (Frazer-Nash)	Technical (Frazer-Nash)	Technical Lead (ENWL)	Technical Lead (ABB)	Technical Lead (AMAT)	Energy Networks Association	Operational Safety Manager (UKPN)	Director of Asset Management (UKPN)
Process / Activity task									
Confirm safety approval process	R	C	I	I	I	I	I	A	I
Define system description / use cases	A	I	R	I	C	C	I	I	I
Identify hazards	A	R	C	I	C	C	I	C	I
Perform risk assessment	A	R	C	I	C	C	I	C	I
Define safety requirements / acceptance criteria	A	R	C	I	C	C	I	C	I
Develop safety claims and arguments	A	R	C	I	C	C	I	C	I
Gather evidence to support safety claims, arguments	A	I	I	I	R	R	I	I	I
Produce PSCR	R	R	C	I	C	C	I	A	C

5.2 SAFETY ORGANISATION

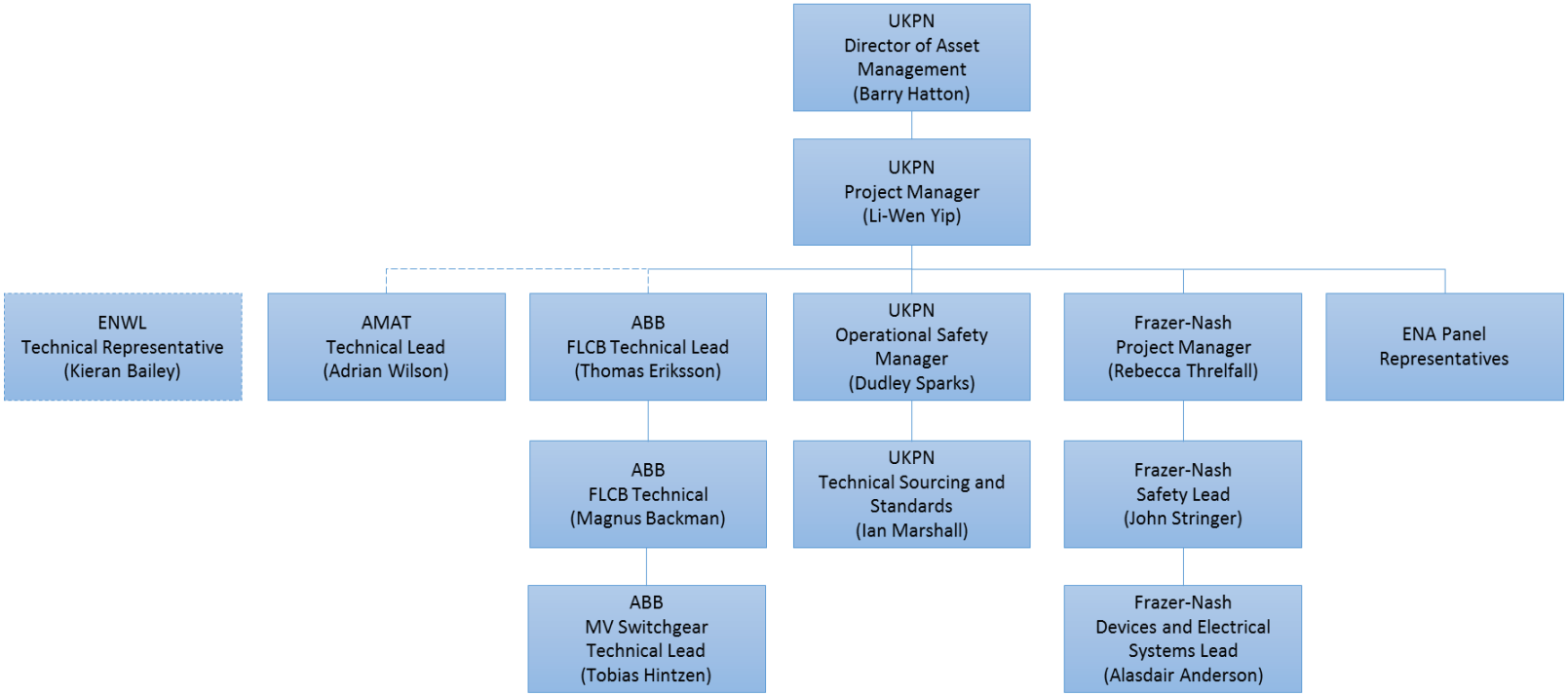

Figure 4: Powerful-CB Safety Organisation Chart

6. SAFETY CASE PRINCIPLES & ACCEPTANCE CRITERIA

6.1 SAFETY CASE PRINCIPLES

The following high level safety case principles have been derived which will be used to determine whether a case for safety has been made for each device. In the absence of a regulatory framework for safety cases on 11kV networks, these principles have been derived from other high hazard industries, namely the Offshore Installations (Safety Case) Regulations [8] and EU Common Safety Method for Risk Evaluation and Assessment (CSM REA) Regulations [9].

SCP 1 The Safety Case should demonstrate that the management system (i.e. policy, organisation, documentation, training, performance monitoring, change control etc.) is adequate to ensure compliance with the relevant statutory provisions and show an appropriate level of control during each phase of the 'system' life cycle (i.e. from initial testing and implementation through to end of life replacement & decommissioning).

SCP 2 The Safety Case should describe how the principles of risk evaluation and risk management are being applied to the design to ensure that risks will be controlled so as to ensure compliance with the relevant statutory provisions.

SCP 3 A systematic process should be used to identify all reasonably foreseeable hazards that apply to the 'system', together with potential initiating events or sequences of events.

SCP 4 The methodology and evaluation criteria adopted for risk assessment should be clear.

SCP 5 The identification of risk reduction measures should be systematic and take into account new knowledge as it arises. Risk reduction measures identified, as part of the risk assessment, should be implemented if they are reasonably practicable.

SCP 6 In deciding what is reasonably practicable, the case should show how relevant good practice and judgement based on sound engineering, management and human factors principles have been taken into account.

SCP 7 Where remedial measures are proposed to reduce risk, the timescale for implementing them should take account of the extent of such risks and any practical issues involved.

SCP 8 Appropriate control and mitigation measures should be provided to minimise the likelihood and an accident and protect personnel from the consequences. Measures and arrangements for controlling an emergency should identified and take account of likely conditions during emergency scenarios.

6.2 TOLERABILITY OF RISK

HSE's Reducing Risks, Protecting People (R2P2) [10] states "In everyday life there are some risks that people choose to ignore and others that they are not prepared to entertain. But there are also many risks that people are prepared to take by operating a trade-off between the benefits of taking the risks and the precautions we all have to take to mitigate their undesirable effects". This is the basis for the Tolerability of Risk (TOR) framework which puts risks into three regions as shown in Figure 5.

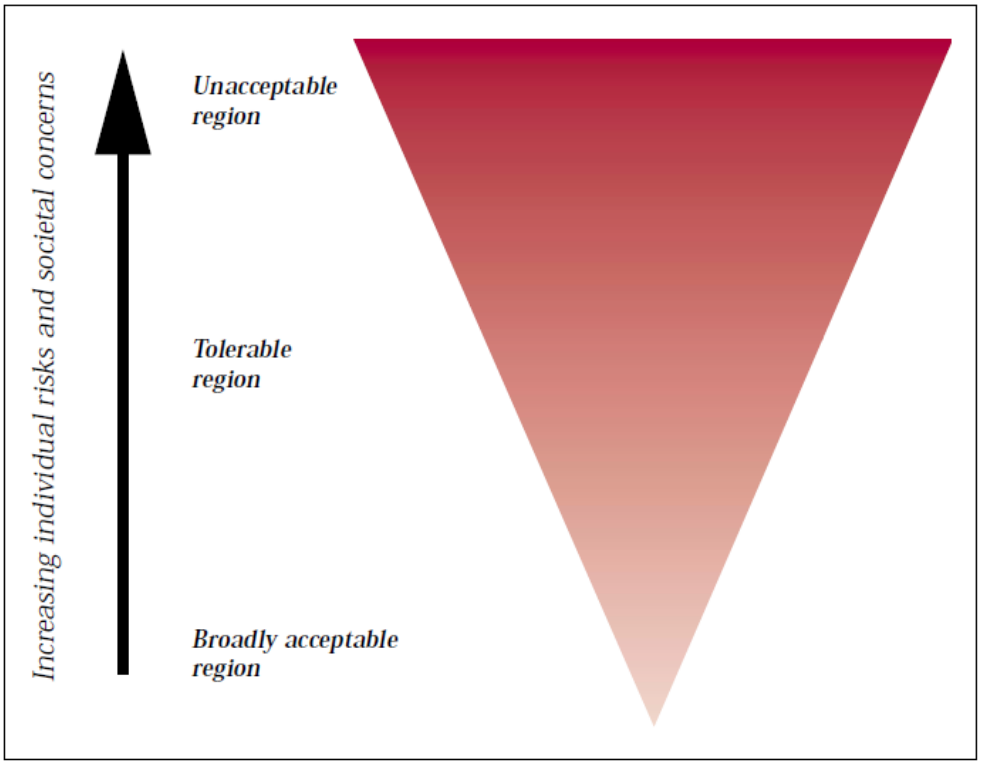

Figure 5: HSE framework for the Tolerability of Risk

For practical purposes, a particular risk falling into the 'Unacceptable' region is regarded as unacceptable whatever the level of benefits associated with the activity and cannot be tolerated under any circumstances. Any activity or practice giving rise to risks falling in that region would, as a matter of principle, be ruled out unless the activity or practice can be modified to reduce the degree of risk so that it falls in one of the regions below.

Risks falling into the 'Broadly Acceptable' region are generally regarded as insignificant and adequately controlled. HSE, would not usually require further action to reduce risks unless reasonably practicable measures are available. The levels of risk characterising this region are comparable to those that people regard as insignificant or trivial in their daily lives. They are typical of the risk from activities that are inherently not very hazardous or from hazardous activities that can be, and are, readily controlled to very low risks. Nonetheless, duty holders must reduce risks wherever it is reasonably practicable to do so or where the law so requires it.

The zone between the unacceptable and broadly acceptable regions is the 'Tolerable' region. Risks in that region are typical of the risks from activities that people are prepared to tolerate in order to secure benefits. The level of risk in this region may be tolerated when it has been demonstrated that the risk is ALARP and is not 'Unacceptable'.

6.3 RISK CLASSIFICATION MATRIX

For the assessment of risk for use of the two FLCB devices on the electricity distribution network a risk classification matrix is used (developed herein from HSE targets) which defines the boundaries between the 'Unacceptable', 'Tolerable' and 'Broadly Acceptable' regions for both the exposed worker (staff or contractors) in Figure 6 and the general public in Figure 7. The 'Unacceptable' region is shown in red, the 'Tolerable' region in yellow and 'Broadly Acceptable' region in green. Where applicable, UKPN Investigation Classifications, as defined in [7] (i.e. Very Serious Incident (VSI), Serious Incident (SI), Incident (I)), are also indicated.

CONSEQUENCE	LIKELIHOOD					
	Very Likely	Likely	Possible	Unlikely	Very Unlikely	Improbable
	$< 10^{-0}\ yr^{-1}$	$< 10^{-1}\ yr^{-1}$	$< 10^{-2}\ yr^{-1}$	$< 10^{-3}\ yr^{-1}$	$< 10^{-4}\ yr^{-1}$	$< 10^{-5}\ yr^{-1}$
Catastrophic	Unacceptable (-)	Unacceptable (-)	Unacceptable (-)	Unacceptable (-)	Tolerable (-)	Tolerable (-)
Critical	Unacceptable (VSI)	Unacceptable (VSI)	Unacceptable (VSI)	Tolerable (SI)	Tolerable (I)	Broadly Acceptable (I)
Major	Unacceptable (SI)	Unacceptable (SI)	Tolerable (SI)	Tolerable (I)	Broadly Acceptable (I)	Broadly Acceptable (I)
Minor	Unacceptable (SI)	Tolerable (SI)	Tolerable (I)	Broadly Acceptable (I)	Broadly Acceptable (I)	Broadly Acceptable (I)
Negligible	Tolerable (I)	Tolerable (I)	Broadly Acceptable (I)	Broadly Acceptable (I)	Broadly Acceptable (I)	Broadly Acceptable (I)

Figure 6: Risk Classification Matrix for Workers

CONSEQUENCE	LIKELIHOOD					
	Very Likely	Likely	Possible	Unlikely	Very Unlikely	Improbable
	$< 10^{-0}\ yr^{-1}$	$< 10^{-1}\ yr^{-1}$	$< 10^{-2}\ yr^{-1}$	$< 10^{-3}\ yr^{-1}$	$< 10^{-4}\ yr^{-1}$	$< 10^{-5}\ yr^{-1}$
Catastrophic	Unacceptable (-)	Unacceptable (-)	Unacceptable (-)	Unacceptable (-)	Unacceptable (-)	Tolerable (-)
Critical	Unacceptable (VSI)	Unacceptable (VSI)	Unacceptable (VSI)	Unacceptable (SI)	Tolerable (I)	Tolerable (I)
Major	Unacceptable (SI)	Unacceptable (SI)	Unacceptable (SI)	Tolerable (I)	Tolerable (I)	Broadly Acceptable (I)
Minor	Unacceptable (SI)	Unacceptable (SI)	Tolerable (I)	Tolerable (I)	Broadly Acceptable (I)	Broadly Acceptable (I)
Negligible	Unacceptable (I)	Tolerable (I)	Tolerable (I)	Broadly Acceptable (I)	Broadly Acceptable (I)	Broadly Acceptable (I)

Figure 7: Risk Classification Matrix for General Public

The consequences in the above risk classification matrices relate to personal injury, property damage and environmental impact. Consequence definitions are provided in Table 2 below, taken from UKPN Incident Reporting procedure [7].

Table 2: Consequence Definitions

Consequence	Personal Injury	Property Damage	Environmental Impact
Catastrophic	Multiple fatalities	Major fire-explosion	Catastrophic impact
Critical	Fatality, terminal ill-health condition or permanent disability	Major damage or loss	High impact
Major	Lost Time Incident	Significant property damage	Medium impact
Minor	Medical Treatment Injury	Short term local damage or loss	Low impact
Negligible	Personal Injury	Very limited property / plant damage or loss	Negligible impact

The risk matrix has been developed specifically for use of the two FLCB devices on the electricity distribution network. This is based on the HSE upper limit of tolerability for individual risk per annum for workers (10^{-3} per year) and for members of the public (10^{-4} per year) [10] and calibrated specifically to the risk associated with the FLCB, accounting for the specific hazards and exposure size in question. The calculation is detailed in Table 3 below.

Table 3: Risk Matrix Calibration

ID	Description	Value	Units	Notes
IR_W	Individual worker risk	10^{-3}	yr^{-1}	Value taken from HSE guidance [10]
P	At risk population	10^{3}	-	It is assumed that approximate 20% of the total UKPN workforce (5000 employees) may be exposed to switchgear as part of their job roles.
RC	Risk contribution	10^{-2}	-	Risk from FLCB devices should not provide a considerable contribution to the overall worker risk. Therefore a value of 1% is considered appropriate.
H	Hazard set	10^{1}	-	It is anticipated that there will be in the order of 10 significant hazards (i.e. leading to fatalities) associated with the use of FLCB on the network.
RD_W	Risk of worker death from FLCB devices	10^{-3}	yr^{-1}	IR_W x P x RC / H (deaths per hazard)

Therefore, as shown in Figure 6 the border between Critical/Possible and Critical/Unlikely equates to a maximum 'Tolerable' risk of worker death of 10^{-3} per year. The target for the public is an order of magnitude greater, and therefore as shown in Figure 7 the border between

Critical/Unlikely and Critical/Very Unlikely equates to a maximum ‘Tolerable’ risk of public death of 10^{-4} per year.

The HSE believes that an individual risk of death of one 10^{-6} per year corresponds to a very low level of risk [10] and therefore defines the boundary between the ‘Broadly Acceptable’ and ‘Tolerable’ regions for members of the public, as shown in Figure 7. The maximum ‘Broadly Acceptable’ risk of worker death is again an order of magnitude higher (i.e. 10^{-5} per year), as shown in Figure 6, recognising the higher levels of risk tolerability for this exposure group. This is equivalent to other similar high hazard industries (e.g. nuclear power stations).

If the likelihood is less than 10^{-7} per year the event is deemed incredible and can be screened out.

6.4 ACCEPTANCE CRITERIA

Safety acceptance criteria for laboratory testing and field trials will be developed from the safety requirements and analysis and evidence derived in support of the two safety cases. The devices will be considered to be ‘Safe’ when the risks have been demonstrated to have been reduced to a level that is ‘Broadly Acceptable’, or ‘Tolerable’ and ALARP, and relevant prescriptive Safety Requirements have been met.

7. REFERENCES

[1] The Health and Safety at Work etc. Act 1974

[2] The Management of Health and Safety at Work Regulations 1999

[3] Electricity at Work Regulations 1989

[4] The Electricity Safety, Quality and Continuity Regulations 2002

[5] Feasibility of safety case for ABB hybrid fault current limiter, FNC 50235/44699R, 2016.

[6] Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013

[7] UKPN, Incident Reporting, HSS-01-051, Version 8.0, 26 April 2016.

[8] Offshore Installations (Safety Case) Regulations 2005

[9] Commission Implementing Regulation (EU) 2015/1136 amending Implementing Regulation (EU) No. 402/2013 on the Common Safety Method for Risk Evaluation and Assessment.

[10] HSE, 2001, Reducing Risks, Protecting People, HSE's decision-making process.

Frazer-Nash Consultancy Ltd
Stonebridge House
Dorking Business Park
Dorking
Surrey
RH4 1HJ

T 01306 885050
F 01306 886464

www.fnc.co.uk

Offices at:
Bristol, Burton-on-Trent, Dorchester,
Dorking,Glasgow, Plymouth, Warrington
and Adelaide