Powerful-CB

SDRC 9.1.3-4
Preliminary Safety Case
May 2018

THE SUNDAY TIMES 25 BEST BIG COMPANIES TO WORK FOR 2018

INVESTORS IN PEOPLE | Gold

UK Power Networks
Delivering your electricity

Project overview

The Powerful-CB (Power Electronic Fault Limiting Circuit Breaker) project aims to demonstrate that Fault-Limiting Circuit Breakers (FLCBs) can enable more Distributed Generation (DG) to connect to fault-level constrained networks.

A power electronic FLCB is a solid-state circuit breaker that operates 20 times faster than traditional vacuum circuit breakers. The fact that it is much faster than a conventional circuit breaker means that by the time the conventional breaker will be called to break the fault, the FLCB will have already opened and removed the fault contribution of the asset it is connected to (incomer transformer, generator etc.). Consequently the impact of additional generation connection on the fault level capacity of a substation can be considered nullified, allowing further generation to be connected without the need of costly reinforcement.

We will be trialling two methods to allow generators to connect to fault-level constrained 11kV networks:

- Method 1 – Installing a device at a primary substation, to allow multiple generators to connect; and
- Method 2 – Installing a device at a customer site, to allow a single generator to connect.

The journey towards a low carbon economy is revolutionising the way we produce, distribute and consume electricity. Whilst we continue to operate and invest in our network to maintain a safe, secure, and sustainable power supply to 8.2 million homes and businesses, we need to make use of smart, flexible, and innovative techniques to ensure delivery of our outputs, minimise the cost impact on consumers, and manage the increased complexity of this low carbon world.

To date we have over 300MW of combined heat and power (CHP) connected to our London network but the ability to connect more may be limited as a result of fault level constraints. The traditional fault level solutions are: an inhibit agreement (therefore restricting output); connection at a higher voltage level; and network reinforcement with the latter two resulting in an expensive connection which may make projects financially unfeasible.

We are transforming our business into a Distribution System Operator[1] to respond to the needs of our customers, both now and in the future, and working with the wider industry to help deliver decarbonisation of the electricity system at the least cost. The Government's Carbon Plan and the Department of Energy & Climate Change (now known as BEIS) Community Energy Strategy report[2] highlight the importance of CHP in achieving the UK's carbon targets. The Mayor of London's target[3] is to generate 25% of London's heat and power requirements locally by 2025. We expect this to encourage CHP and district heating for new developments.

[1] http://futuresmart.ukpowernetworks.co.uk/
[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/275163/20140126Community_Energy_Strategy.pdf
[3] https://www.london.gov.uk/what-we-do/planning/london-plan/current-london-plan/london-plan-chapter-five-londons-response/poli-0

1 Executive Summary

This is the second Powerful-CB Successful Delivery Reward Criteria (SDRC) report. It presents the independently produced preliminary safety case report for the two methods to trial FLCB introduction to the UK Power Networks (UKPN) network. The purpose of the safety case and the work involved during its production is to define and justify the acceptable levels of risk, analyse failure modes and effects, detail proposed mitigations and provide claims, arguments and evidence to demonstrate that the proposed mitigations reduce the overall level of the risk to an acceptably low level.

UKPN has the best safety record out of all DNOs[4] indicating the prioritisation and importance placed in the area of safety. The same high safety requirements approach will be maintained throughout the Powerful-CB project. In order to have an independent review for the safety case, a third party was sought. Following a set tendering process, Frazer-Nash Consultancy (FNC) were chosen to produce the safety report. All the necessary support from UKPN subject matter and safety experts was provided to FNC. Additionally UKPN provided the required evidence for the support of the report. The project partners (ABB and AMAT) contributed the required information for the production of the safety report. Separate reports were produced for the two different devices to be trialled, and a combined bank of evidence has been compiled to support the safety case. Some of the evidence supporting the safety case are confidential and will be only supplied to Ofgem. The table of evidence in Appendix C of this document provides information about the documents in the bank of evidence.

The NIC Successful Delivery Reward Criteria, which are met by this document as originally set in the Powerful-CB Project Direction by Ofgem, are:

Successful Delivery Reward criterion	**Evidence**
9.1.3 Independent review of safety case	**Issue preliminary safety case to relevant ENA panel(s) for independent review** which will include: Definition and justification of acceptable levels of risk; analysis of failure modes and effects; details of proposed mitigations; and claims, arguments, and evidence to demonstrate that the proposed mitigations reduce the overall level of risk to an acceptably low level. (31 May 2018)
9.1.4 Safety case for FLCB installation without back-up	**Publish preliminary safety case** which will include the technological and operational safety case to the time when the trial equipment could be deployed as BAU without the FLCBs being installed in series with a back-up circuit breaker. (31 May 2018)

This report explains the technical challenges for the use of FLCBs and sets the safety case process and principles for the trials and the future Business As Usual (BAU) adoption of the devices. Furthermore, a rational supporting argument structure for the safety of the device is explained in the document. The evidence setting the foundation for the argument are collated in a table of evidence at the end of the report. In the process of developing this preliminary safety case, a number of documents have been identified that will be produced during the course of the trials. Appendix C includes the bank of evidence that will be required at the time of BAU implementation. For documents which are not yet produced, an indicative timeline is given to indicate this.

"The overall safety argument for the FLCB device is expressed using a "Claims, Argument and Evidence" (CAE) structure. 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, will result in the FLCB device having an acceptable level of safety. 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."

Frazer-Nash Consultancy

[4] https://www.ukpowernetworks.co.uk/internet/en/about-us/documents/6955%20ED1%20report%202017%2010%20INT%20final.pdf?track=ED-final

A BAU implementation of an FLCB on the network would mean that there would not be a conventional back-up circuit breaker in series with the FLCB and additionally the fault levels would be allowed to rise above the conventional switchgear's rating. The safety case presented in this document was produced with the consideration of such a future BAU scenario. However, the purpose of the trials is to initially test the devices on our network and confirm their characteristics on a realistic environment outside of lab conditions. As such, the devices and network will not be put into undue risk of operation. Consequently, the failure mitigation requirements for the trials are lower than BAU. Nevertheless, the safety report will set the safety argument for a future where FLCBs are BAU and the safety requirements are higher.

UKPN present the preliminary safety case, in the form of independent documents attached as appendices – as produced by FNC. Ultimately the Safety Case demonstrates that the devices and their use in both trials and general application is 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 the relevant prescriptive Safety Requirements have been met.

2 Table of contents

1 Executive Summary 3
2 Table of contents 5
3 Glossary and abbreviations 6
4 About us 9
5 Introduction 10
6 Approach and Methodology 12
Appendix A. FNC Preliminary Safety Case Report for Method 1 13
Appendix B. FNC Preliminary Safety Case Report for Method 2 14
Appendix C. Table of Evidence 15

3 Glossary and abbreviations

Term	Description
ABB	ABB Group
Accident	An unintended event, or sequence of events, that causes harm.
ALARP	As Low As Reasonably Practicable
AMAT	Applied Materials Inc.
BAU	Business As Usual
CAE	Claims, Arguments and Evidence
CBA	Cost Benefit Analysis
CB	**Circuit Breaker** – protection device that interrupts the flow of current in an electric circuit in the event of a fault.
CHP	**Combined Heat and Power** – simultaneous generation of usable heat and power (usually electricity) in a single process; more efficient than generating heat and power separately.
Claim	An assertion that contributes to the safety argument.
Consequence	The outcome, or outcomes, resulting from an event.
DG	**Distributed Generation** – generators that are connected to the distribution network.
DNO	Distribution Network Operator
EPN	Eastern Power Networks
Evidence	Records, statements, facts or other information, which are relevant to the audit criteria and verifiable.
Fault Current	A surge of energy that flows through the network in the event of a fault. The energy comes from the momentum of rotating generators and motors connected to the network.
Fault Level	The maximum fault current that could theoretically flow during a fault. **"Make"** fault level is the maximum fault current that could flow during the first current peak of the fault, and that a circuit breaker closing onto a fault would need to safely handle. **"Break"** fault level is the maximum fault current that could be flowing 100ms after the start of the fault, and that a circuit breaker clearing the fault would need to be able to interrupt.
Fault Level Headroom	The difference between fault level and fault rating at a particular substation or part of the network; corresponding to the amount of generation that can be connected to the network without exceeding its fault rating.
FCL	**Fault Current Limiter** – a FLMT that attenuates fault current by increasing its impedance (only) during a fault.
FCS	Fast Commuting Switch
FLCB	**Fault Limiting Circuit Breaker** – a FLMT that blocks fault level contributions from a transformer / bus coupler / generator by disconnecting it before the first current peak of the fault.
FLMT	**Fault Level Mitigation Technology** – a technical solution that reduces fault levels on the network.

Term	Description
FMEA	Failure Mode and Effects Analysis
FSP	Full Submission Proforma
FWI	Fatality and Weighted Injury
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.
HAZID	Hazard Identification
HAZOP	Hazard and Operability Study
HSE	Health and Safety Executive
IBGTs	Insulated Bipolar Gate Transistors
Inhibit / Intertrip Scheme	A hard-wired protection system that automatically disconnects generators from the network under pre-defined conditions, typically in the event of a transformer outage or other abnormal network configuration that causes elevated fault levels.
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.
LPN	London Power Networks
M1	Method 1 - Installation of a FLCB at a substation.
M2	Method 2 - Installation of a FLCB at a customer's premises.
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.
NIC	Network Innovation Competition
Ofgem	Office of Gas and Electricity Markets
Personal Injury	A work-related injury of a minor nature and where the injured person receives no more than first aid treatment either whilst at work or from a medical professional but does not result in a lost time injury.
PFD	Probability of Failure on Demand
PSCR	Preliminary Safety Case Report
RA	Risk Assessment
RIDDOR	Reporting of Injuries, Diseases and Dangerous Occurrence

Term	Description
RIIO-ED1	The current electricity distribution regulatory period, running from 2015 to 2023
Risk	Combination of the likelihood of harm and the severity of that harm.
Risk Reduction	The systematic process of reducing risk.
Rotating DG	A generator that converts mechanical energy to electrical energy using a synchronous AC rotating alternator, e.g. CHP and diesel standby generators. These types of generators have a much larger impact on fault levels than inverter-connected generators e.g. solar PV.
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.
SCP	Safety Case Principles
SDRC	Successful Delivery Reward Criteria
SPN	South Eastern Power Networks
SQEP	Suitably Qualified and Experienced Personnel
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.
UKPN	UK Power Networks

4 About us

UKPN provides electricity to 18 million people (8.2 million homes and businesses); 28% of the United Kingdom's population[4], via its electricity distribution networks and is committed to:

- Maintaining a safe, secure and sustainable power supply to over eight million homes and businesses in London, the South East and the East of England;
- Developing what is already Britain's biggest electricity network – including over 112,000 11kV secondary circuit breakers;
- Strengthening our links with the local communities we serve and building on the skills base of the 6,500 people who work for us across the network; and
- Giving our customer the best possible service and maintaining operational efficiency across our network areas.

We have a clear vision to be the best performing Distribution Network Operator (DNO) in the UK over the 2015/16 to 2018/19 regulatory period, the first four years of RIIO-ED1. We will achieve this by demonstrating industry leadership in the three areas below:

- The safest
- The best employer

- The most reliable
- The best service
- **The most innovative**
- The most socially and environmentally responsible

- The lowest cost

Our innovation strategy supports our corporate vision, which underpins our mission and provides clarity of purpose. A key success indicator in delivering our vision is to be classed as the "Most Innovative DNO"; as such it is core to how we do business. A successful innovation programme will support all three elements of our corporate vision; for example innovation is a central component of our strategy continuing to be the lowest cost electricity distributor. Our innovation focus areas outline the objectives of innovation – showing why we innovate.

5 Introduction

Distributed generation (DG) is a vital enabler of the low carbon transition. The decarbonisation of heat is a key element of the Government's Carbon Plan[5]. A key enabler of this decarbonisation is the growth of district heating and DG in the form of combined heat and power (CHP). However, fault level constraints are becoming a barrier to connecting new DG in urban areas. With plans for increased local generation, especially CHP, the already limited headroom in substations will be quickly exhausted.

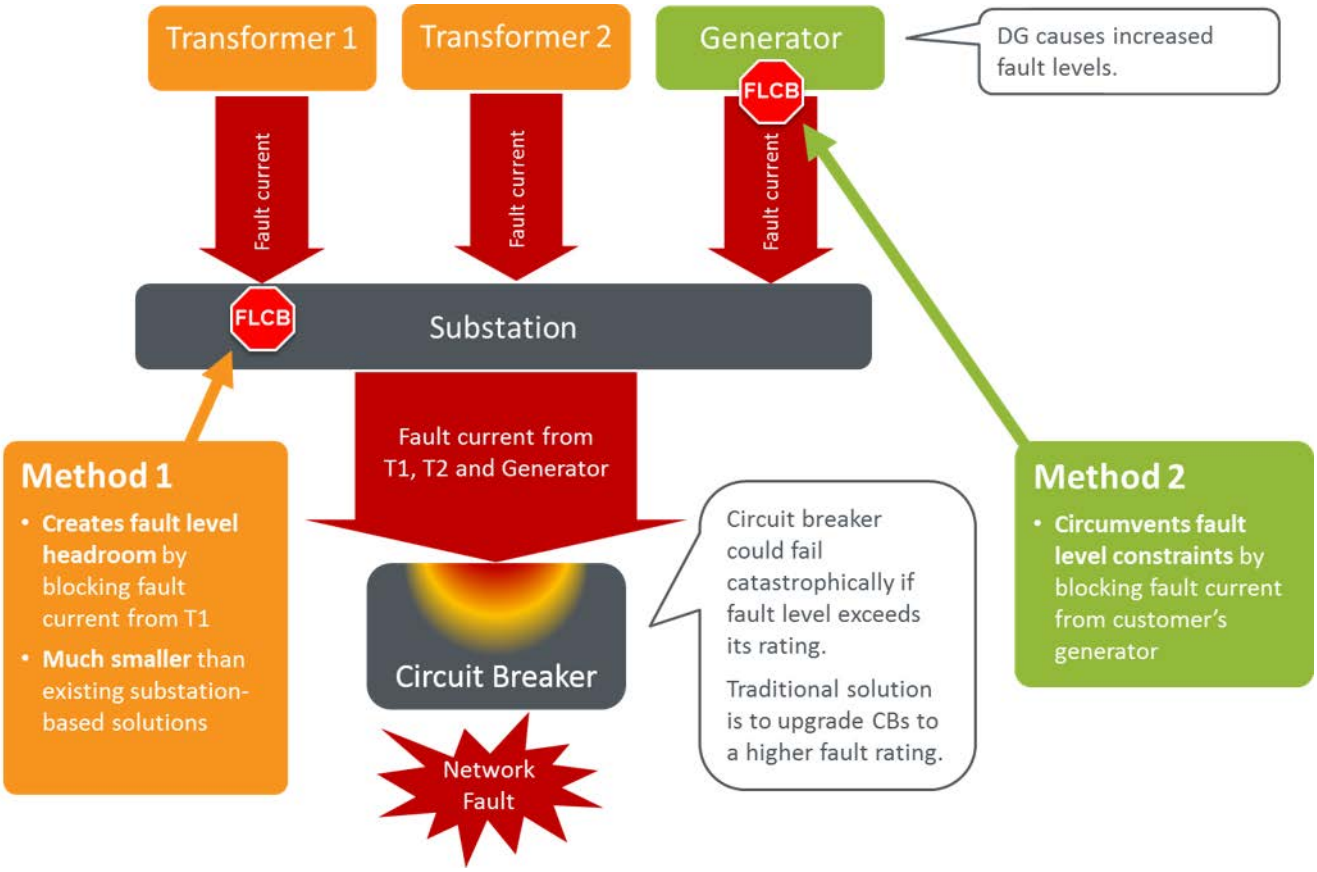


Figure 1 Powerful-CB trials concept

Powerful-CB aims to increase the range of fault level mitigation technologies (FLMTs) available to DNOs and customers. Existing FLMTs have not been adopted widely due to a number of factors including large space requirement and power losses. The project will give generation customers two new options to achieve quicker and more cost-effective connections to fault-level-constrained networks. The safe operation of the network is always the highest priority, we take caution in introducing new products to our networks and therefore a safety case report is required. Due to the innovative aspect of this project and the fact that the plant is under development at the time of writing this paper (Figure 2), a preliminary safety case report is presented in this SDRC according to the section 9 of NIC submission[6]. The purpose of the preliminary safety case is to set the safety case plan for the trials and BAU, collect all the currently available supporting evidence and set target evidence to be produced prior, during and after the trials. Following the trials, a large body of evidence will be available to build upon the safety principles set in this preliminary report. The result will be the complete safety report for the adoption of the Powerful-CB developed technologies.

[5] https://www.gov.uk/government/publications/the-carbon-plan-reducing-greenhouse-gas-emissions--2
[6] https://www.ofgem.gov.uk/system/files/docs/2016/11/powerful-cb_nic_fsp_resubmission_2016-10-20-1700_non-confidential.pdf

In order to maintain an independent view of the project safety case, an external partner was sought for the production of the preliminary safety case. As per industry procurement standard practice, a tender process was followed to achieve optimal results. A request for proposal including the safety case scope and project plan was sent to six companies and three expressed their interest by submitting proposals. The remaining three declined to participate in the tender.

The submissions were evaluated based on three criteria.

1. The experience of the company
2. The amount of detail provided in the proposed methodology and plan
3. The cost of producing the safety report and the detailing of the scope

Based on overall score, the recommended option was Frazer-Nash Consultancy (FNC). A similar procurement strategy was followed for the production of the initial study on the feasibility of safety case for FLCBs, with FNC being the successful bidder. The success of FNC in both events is attributed to the fact their proposal was the most detailed one, offering the best overall balance of available personnel and total cost.

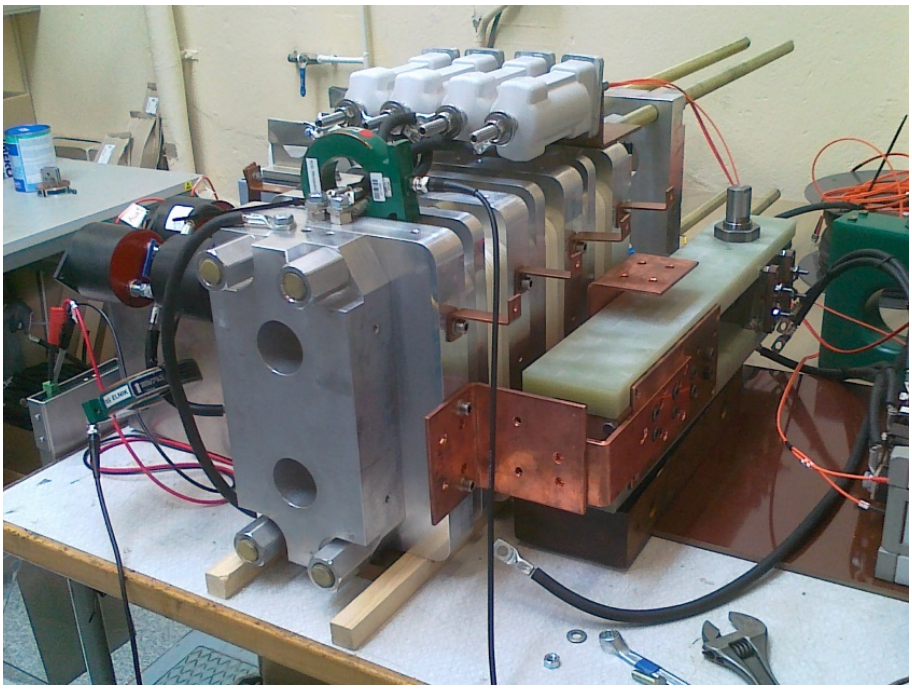


Figure 2 FLCB under development for Method 1

A phased approach was adopted for the production of the preliminary safety report. The fact that FNC had produced the initial feasibility of the safety case submitted as part of the FSP for the Powerful-CB project, allowed for the extra benefit of faster integration to the project. This preliminary safety case report is the first of three phases. The first phase's target and outcome is to develop the safety acceptance criteria for the laboratory testing and field trials of the FLCBs. The second phase will include the findings and results from commissioning and field trials. The third and final phase shall include the findings and learning experiences gained from the trial and use of FLCBs on the live network. During the entire process of developing the phase one safety report of the project, FNC engaged with key stakeholders with the support of the Innovation Team. The list of phases is:

- Phase 1: Preliminary safety case (Appendix A & Appendix B in this SDRC); produced prior to the development of the device
- Phase 2: Safety case for the trials; phase 1 plus evidence produced prior to initiation of FLCB installation works
- Phase 3: Safety case for the usage of FLCB as BAU; phase 2 plus evidence produced after the completion of trials

6 Approach and Methodology

With FNC on-board, a hazard identification workshop was held with to identify all reasonably foreseeable hazards. A major requirement was to identify the suitably qualified and experienced persons (SQEP) within the business and academia. The process and parameters to identify hazards were set before the actual workshop. A separate workshop for each method was conducted and findings are collated in the workshop reports.

This preliminary safety case report has an outlook for the future introduction of FLCBs as BAU and sets the required evidence for such a case. However the initial scope of the trial is to prove the device, consequently, it will be tested on a network arrangement where fault levels do not exceed the fault ratings of conventional equipment, and thus the risks are lower. We have considered both of these scenarios as part of this preliminary safety case and will continue to do so as we progress through the phases. Nonetheless, additional design considerations were taken due to the fact that the device to be trialled is new to the network. For example, the company's subject matter experts instructed that it would be necessary to have the ability to isolate the device from the network by using conventional proven equipment. The design improvement to satisfy that requirement increased the overall safety of the trials.

The safety case is structured on a hierarchical structure of claims, arguments and evidence, in which the:

- Claims are the high level goals for the overall safety of the device;
- Arguments are supporting statements and their purpose is to explain the goals; and
- Evidence can be a variety of documents including testing reports, safety workshop reports, strategy documents and training materials.

Therefore, a body of evidence has been built up as part of the work for the production of the preliminary safety case report. Some of the evidence is confidential, and as such there will be two versions. One version will be publicly available and one will be released to Ofgem only. Moreover the document indicates the evidence that will be produced during the project's lifetime in order to support the final safety case for FLCBs.

Future actions will be required to prepare the necessary safety evidence before the commencement of construction, commissioning and trialling processes. As the final device development stages are reached, more information will become available. This information and collaborative action between the suppliers and UKPN will result in the production of the required evidence.

One report for each Method was produced by FNC with UKPN providing input when required as per the original scope. Appendix A holds the preliminary safety case report for the ABB produced prototype as used in Method 1. Appendix B holds the preliminary safety case report for the AMAT produced prototype as used in Method 2.

Appendix A. FNC Preliminary Safety Case Report for Method 1

The exact copy of the report is attached at the end of this document. No modifications have been done to the FNC produced report. The reference number for the document is FNC 52680/47044R.

Appendix B. FNC Preliminary Safety Case Report for Method 2

The exact copy of the report is attached at the end of this document. No modifications have been done to the FNC produced report. The reference number for the document is FNC 52680/47045R.

Appendix C. Table of Evidence

The status of each piece of evidence is defined as:

- Green – A complete issued version of the evidence is held;
- Yellow – A draft version or a reference to the evidence is held; and
- Orange – No evidence currently exists, but will be produced in the future.

Table 1 Safety Case Evidence Table

ID	Privacy	ABB – Method 1				AMAT – Method 2			
		Reference	Document Title	Issue / Date	Status	Reference	Document Title	Issue / Date	Status
E1	Public	FNC 52680-96871V	Powerful-CB HAZID Workshop Briefing Note	Issue 1 Jun-17	G	FNC 52680-96871V	Powerful-CB HAZID Workshop Briefing Note	Issue 1 Jun-17	G
E2	Chapter 3.2 Ofgem	FNC 52680-46196R	Powerful-CB HAZID Workshop Report (ABB)	Issue 1 Aug-17	G	FNC 52680-46195R	Powerful-CB HAZID Workshop Report (AMAT)	Issue 1 Aug-17	G
E3	Public	FNC 52680-98445V	Powerful-CB Hazard Record (ABB)	Issue 2 Apr-18	G	FNC 52680-98446V	Powerful-CB Hazard Record (AMAT)	Issue 2 Apr-18	G
E4	Public	FNC 50235-44699R	Feasibility of safety case for ABB hybrid fault current limiter	Issue 1 Aug-16	G	N/A	N/A	N/A	N/A
E5	Public	FNC 52680-45804R	Powerful-CB Safety Case Process and Principles	Issue 1 May-17	G	FNC 52680-45804R	Powerful-CB Safety Case Process and Principles	Issue 1 May-17	G
E6	Public	FNC 52680-46624R	Powerful-CB Risk Assessment Workshop Report	Issue 1 Nov-17	G	FNC 52680-46624R	Powerful-CB Risk Assessment Workshop Report	Issue 1 Nov-17	G
E7	Public	FNC 52680-98714V	Powerful-CB Risk Assessment Workshop Briefing Document	Issue 1 Sep-17	G	FNC 52680-98714V	Powerful-CB Risk Assessment Workshop Briefing Document	Issue 1 Sep-17	G

ID	Privacy	ABB – Method 1				AMAT – Method 2			
		Reference	Document Title	Issue / Date	Status	Reference	Document Title	Issue / Date	Status
E8	Ofgem	Non specific	ABB Powerful CB Implementation	Rev 1 Apr-18	G	TBC: Prior to trials	AMAT FLCB Design Report	TBC: Prior to trials	O
E9	Ofgem in parts	TBC: Prior to trials	ABB FLCB Testing and Commissioning Report	TBC: Prior to trials	O	TBC: Prior to trials	AMAT FLCB Testing and Commissioning Report	TBC: Prior to trials	O
E10	Ofgem in parts	TBC: After the trial	Powerful-CB ABB FLCB Trial Reports	TBC: After the trial	O	TBC: After the trial	Powerful-CB AMAT FLCB Trial Reports	TBC: After the trial	O
E11	Public	TBC: Prior to trials	Installation Strategy Report	TBC: Prior to trials	O	TBC: Prior to trials	Installation Strategy Report	TBC: Prior to trials	O
E12	Public	TBC: During the trial	Network Installation and Commissioning Report	TBC: During the trial	O	TBC: During the trial	Network Installation and Commissioning Report	TBC: During the trial	O
E13	Public	TBC: Prior to trials	Resource Plan for Trial and BAU	TBC: Prior to trials	O	TBC: Prior to trials	Resource Plan for Trial and BAU	TBC: Prior to trials	O
E14	Public	TBC: After the trial	Training and Competence Plan	TBC: After the trial	O	TBC: After the trial	Training and Competence Plan	TBC: After the trial	O
E15	Public	TBC: After the trial	Assurance Management System Document	TBC: After the trial	O	TBC: After the trial	Assurance Management System Document	TBC: After the trial	O
E16	Public	TBC: After the trial	Infrastructure Report	TBC: After the trial	O	TBC: After the trial	Infrastructure Report	TBC: After the trial	O
E17	Public	N/A	N/A	N/A	N/A	TBC: Prior to trials	AMAT FLCB Device Equipment Reference Manual	TBC: Prior to trials	O
E18	Public	HSS-01-051	UKPN Incident Reporting Procedure	Version 8.0 Apr-16	G	HSS-01-051	UKPN Incident Reporting Procedure	Version 8.0 Apr-16	G
E19	Public	FNC 52680-46624R	Powerful-CB Risk Assessment Workshop Report	Issue 2 May-18	G	FNC 52680-46624R	Powerful-CB Risk Assessment Workshop Report	Issue 2 May-18	G

ID	Privacy	ABB – Method 1				AMAT – Method 2			
		Reference	Document Title	Issue / Date	Status	Reference	Document Title	Issue / Date	Status
E20	Ofgem (in parts)	TBC: Prior to trials	ABB Reliability Data and FMEA Report	TBC: Prior to trials	O	TBC: Prior to trials	AMAT 250A FLCB Device Reliability Data and FMEA Report	TBC: Prior to trials	O
E21	Ofgem	ETS 03-6511	Standard for Indoor 12kV Power-Electronic Fault-Limiting Circuit Breakers	Version 1.1 Jun-17	G	ETS 03-6511	Standard for Indoor 12kV Power-Electronic Fault-Limiting Circuit Breakers	Version 1.1 Jun-17	G
E22	Ofgem	ETS 03-6510	Standard for Indoor 12kV, 24kV and 36kV Metal Enclosed Switchgear for Grid and Primary Substations	Version 5.0 Aug-17	G	ETS 03-6510	Standard for Indoor 12kV, 24kV and 36kV Metal Enclosed Switchgear for Grid and Primary Substations	Version 5.0 Aug-17	G

Powerful-CB

Preliminary Safety Case Report- ABB FLCB Device

FNC 52680/47044R Issue 1

Prepared for UK Power Networks

SYSTEMS AND ENGINEERING TECHNOLOGY

DOCUMENT INFORMATION

Project : Powerful-CB

Report Title : Preliminary Safety Case Report- ABB FLCB Device

Client : UK Power Networks

Client Ref. : 7600003478

Classification :

Report No. : FNC 52680/47044R

Issue No. : 1

Date : 14-May-2018

Compiled By : Jamie Moore

Verified By : John Stringer

Approved By : Stephen Clark

Signed :

DISTRIBUTION

Copy	Recipient	Organisation
1	Laura Daniels	UK Power Networks
2	John Moutafidis	UK Power Networks
3	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

EXECUTIVE SUMMARY

This Preliminary Safety Case Report (PSCR) presents the overall safety argument for the ABB 2000A Fault Limiting Circuit Breakers (FLCB) in a 'Claims, Arguments and Evidence (CAE)' structure. Each claim is supported by multiple arguments and a set of robust evidence.

The electricity network is inherently dangerous due to the large amounts of electrical power being transported through it. Under certain conditions this power can become uncontrolled and cause damage to equipment and injury to people. In order to reduce the likelihood of such occurrences, the risks have been eliminated or controlled as far as reasonably practicable. This is underpinned by the Distribution Network Operators legal obligation to ensure the safe operation of their electricity network.

In the current state of the network, the risks associated with switchgear are well known and managed. Following Hazard Identification (HAZID) and Risk Assessment (RA) workshops, the likelihood of either a flashover / local explosion or electric shock as a result of a fault with the FLCB device was assessed against the present risk with the currently installed circuit breakers and it was agreed that the use of the FLCB device did not give an increased risk compared to the current network. Therefore, on the basis that the risk is no different to what is already accepted on the network, it can be considered to be 'Broadly Acceptable'.

However, the application for which the FLCB is used is new and unique to the electricity network, as it allows the potential fault currents to exceed the ratings of some network equipment. This is the additional risk that is created by the FLCB project and this safety case ultimately argues whether it can be reduced to Tolerable or ALARP.

During the trials the potential fault current limit of the network will not be exceeded, therefore the potential safety measures identified at the RA workshop to mitigate this are not required. In addition, the FLCB will have adjacent conventional circuit breakers. Therefore the risk can be considered to be no worse than existing substations in operation and the protection design is beyond the current practice.

A BAU (Business As Usual) implementation of an FLCB on the network would mean that there would not be a conventional back-up circuit breaker in series with the FLCB and additionally the fault levels would be allowed to rise above the conventional switchgear's rating. Therefore in BAU, switchgear exposure to excessive fault current could lead to disruptive failure and potentially result in an explosion within the sub-station, leading to fire if an oil circuit breaker is present. A risk assessment was undertaken to assess the tolerability of this risk and a Cost Benefit Analysis (CBA) was undertaken on various potential Safety Measures to support a decision as to whether these risks are As Low As Reasonably Practicable (ALARP) Safety Measure. The analysis concluded that, due to the high reliability of the devices, the safety risk is tolerably low and the cost to implement any of the three potential Safety Measure options is grossly disproportionate to the safety benefit gained. This will be reviewed following the trial and further system studies may be undertaken in the future for the use of FLCBs in BAU scenarios where the fault capacity might be exceeded.

The high reliability of the device is crucial to the validity of this analysis and thus the safety case. A key Safety Requirement was therefore derived from the CBA for the Probability of Failure on Demand (PFD) of the ABB device to be less than $1x10^{-3}$. The certification of the design of the device proving the reliability is a key part of the evidence and is used to support the claim that "the FLCB device is designed to operate effectively and safely for all postulated network fault conditions and satisfies the derived Safety Requirements" (Claim C2).

The results of the trial will also further influence the design and development of maintenance schedules and operator instructions. These will be used to revalidate and update elements of the safety case prior to extended operations and ultimately BAU operation.

In summary this PSCR concludes that:

1. The hazards associated with the FLCB device are understood and sufficiently managed such that the operation and implementation of the device at the trials site can be considered to be ‘Safe’, whereby the risks have been reduced to a level that is either ‘Broadly Acceptable’ or ‘Tolerable and ALARP’.
2. Provided that the reliability of the FLCB device can be proven during the trial period, and that the risks associated with construction / installation are understood and will be adequately controlled, a suitable ‘case for safety’ can be made for operation of the FLCB device in BAU application such that the safety risks associated with the network equipment seeing a fault current above its rating can be ‘Broadly Acceptable’ or that the risk can be reduced to be ‘Tolerable’ and ‘ALARP’.

This PSCR has been produced to support both the trial and the BAU application. A number of evidence items, e.g. those to be generated during the trial, remain outstanding at the time of this issue. Where this is the case this has been highlighted in blue. Following the trial this PSCR will be updated and the CAE will be revisited to support BAU application.

ACRONYMS AND ABBREVIATIONS

ABB	ABB Group
ALARP	As Low As Reasonably Practicable
AMAT	Applied Materials Inc.
BAU	Business As Usual
BiGT	Bi-mode Insulated Gate Transistor
CAE	Claims, Arguments and Evidence
CBA	Cost Benefit Analysis
DG	Distributed Generation
DNO	Distribution Network Operator
EPN	Eastern Power Networks
FCS	Fast Commuting Switch
FLCB	Fault Limiting Circuit Breakers
FMEA	Failure Mode and Effects Analysis
FWI	Fatality and Weighted Injury
HAZID	Hazard Identification
HAZOP	Hazard and Operability Study
HSE	Health and Safety Executive
IBGTs	Insulated Bipolar Gate Transistors
LPN	London Power Networks
NIC	Network Innovation Competition
PFD	Probability of Failure on Demand
PSCR	Preliminary Safety Case Report
RA	Risk Assessment
RIDDOR	Reporting of Injuries, Diseases and Dangerous Occurrence
SCP	Safety Case Principles
SPN	South Eastern Power Networks
SQEP	Suitably Qualified and Experienced Personnel
UKPN	UK Power Networks

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 no more than first aid treatment either whilst at work or from a medical professional but does not result in a lost time injury.
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 8
1.1 BACKGROUND 8
1.2 SAFETY CASE REQUIREMENT 8
1.3 DOCUMENT PURPOSE 9

2. SCOPE OF THE SAFETY CASE 10

3. SYSTEM DESCRIPTION / USE CASES 11
3.1 TECHNICAL CHALLENGE 11
3.2 ABB 2000A FLCB 11
3.3 TRIAL 12

4. SAFETY CASE PROCESS AND PRINCIPLES 14
4.1 SAFETY MANAGEMENT PROCESS 14
4.2 SAFETY CASE PRINCIPLES 14
4.3 ACCEPTANCE CRITERIA 15

5. SAFETY CLAIMS, ARGUMENTS AND EVIDENCE 16
5.1 OVERVIEW 16
5.2 CLAIM C1 – SAFETY REQUIREMENTS 17
5.3 CLAIM C2 – FLCB DESIGN 22
5.4 CLAIM C3 – IMPLEMENTATION 25
5.5 CLAIM C4 - OPERATION 26
5.6 EVIDENCE SUMMARY 28

6. CONCLUSIONS 29

7. REFERENCES 30

ANNEX A - CLAIMS, ARGUMENTS, EVIDENCE DIAGRAMS 31

ANNEX B - SAFETY CASE EVIDENCE TABLE 37

ANNEX C - FLCB DEVICE SPECIFICATION 39

1. INTRODUCTION

1.1 BACKGROUND

Fault current limiting technologies can be used to solve the fault level constraints, presented by interconnection, short cable distances and other factors, which are limiting the growth of low-carbon generation on electricity distribution networks in Great Britain. Fault Limiting Circuit Breakers (FLCBs) provide a means to allow the continued growth and connection of Distributed Generation (DG) onto the distribution network in a cost-effective manner.

In developing the safety argument for the ABB 2000A FLCB it is important to recognise that operation of the existing 11kV distribution network is not free from risk as there is the potential for arcing / flashovers or electric shock etc. from existing switchgear. These risks are well known and already managed and the introduction of the FLCB device is not expected to adversely affect them. However, the FLCB device does introduce a new safety risk in that, with increased Distributed Generation (DG), there is the potential for network equipment to experience a fault current above its rating should the FLCB fail to operate on demand. The safety case presented herein considers this 'additional' risk and ultimately argues whether the risk can be reduced to be 'Tolerable and ALARP'.

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

- The first device, produced by ABB, is designed for deployment in primary substations.
- The second, produced by Applied Materials (AMAT), is designed for direct connection to customer generators.

Parallel trials are being undertaken to provide an insight to stakeholders on the relative suitability of the two technologies, each in a suitable location, as well as provide 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.

The first device, produced by ABB, will be trialled at a primary substation and the second, produced by AMAT, at a customer generator site. The trials will not exceed the fault level limit however this scenario is a possibility in BAU. The risks associated with running the substation with fault levels above what the equipment is rated for are higher. Therefore the devices will need to be verified that they can reliably operate as described by the manufacturer before the devices can be extended from the trial to general use. For more details around the Annex C of this report.

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 also demonstrates that the safety management system (i.e. policy, organisation, documentation, training, performance monitoring, change control etc.) are 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, the Safety Case is 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 for BAU.

Development of the Safety Case 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 present the safety argument for the ABB 2000A FLCB device to support the trials and to provide confidence that a ‘case for safety’ can be made for the BAU application.

2. SCOPE OF THE SAFETY CASE

Operation of the existing 11kV distribution network is not free from risk as there is the potential for arcing / flashovers or electric shock etc. from existing switchgear. These risks are well known and managed and are considered to be 'Broadly Acceptable'. Introduction of the ABB FLCB device is not expected to adversely affect this. However, the application for which the FLCB device is used is new and unique to the electricity network which introduces a new risk as it allows the potential fault currents to exceed the ratings of some network equipment.

The scope of the Safety Case is bound by the FLCB device itself, its functionality and the environment it will operate in. Initially, this will be constrained to a trial at one specific site but it also considers BAU operation on the wider 11kV network (i.e. a generic application case) in order to ensure that the Safety Case is comprehensive. This has been developed as part of the Safety Management process (see Section 4).

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 FLCB 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 demonstrates that the devices and their use in both trials and general application is 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 the relevant prescriptive Safety Requirements have been met. Adherence to the safety case principles (see Section 4.2) is used to determine whether a suitable 'case for safety' has been made.

3. SYSTEM DESCRIPTION / USE CASES

3.1 TECHNICAL CHALLENGE

A conventional circuit breaker interrupts fault current by physically separating its contacts, allowing the resulting voltage surge to form an arc between the contacts, then using various methods to extinguish the arc. A typical vacuum circuit breaker takes 40-60ms to open its contacts, then another 10-15ms to extinguish the arc, for a total interruption time of 50-75ms.

Conversely, a power electronic FLCB interrupts fault current by turning off Insulated Bipolar Gate Transistors (IBGTs), and uses a surge arrestor to absorb the voltage surge without forming an arc The Fast Commutating Switch opens while the IBGTs are conducting and therefore at the point of interruption of the current there are no moving parts, so the fault current can be interrupted within 2ms or less.

Existing FLCB technologies suffer from limitations caused by conduction losses, as the IBGTs that interrupt fault current also have to carry normal load current. This means that the current FLCBs need many IBGT modules to handle the current at full load; and/or need a large cooling system to dissipate heat at full load. Space requirements for existing FLCBs prevent their usage at London Power Networks (LPN) substations where space is usually limited and therefore block their consideration as a viable alternative to the proposed scheme.

The trial will be carried out on the LPN. However, as previously mentioned and following a successful outcome, BAU installation may include installation onto the Eastern Power Networks (EPN) and the South Eastern Power Networks (SPN).

3.2 ABB 2000A FLCB

ABB is a global leader in power and automation technologies with a long tradition in developing state of the art technologies and products. They have a solid track record of working on Low Carbon Networks Fund / NIC projects involving power electronics and fault level solutions.

ABB's 2000A FLCB solution eliminates conduction losses by using an innovative "fast commutating switch" (FCS) that bypasses the power electronics during normal operation, and opens within 0.35ms in the event of a fault. This eliminates the need for a bulky cooling system, making this technology feasible to install in an existing indoor substation.

ABB propose that this prototype can be housed in three 1000mm-wide modular switchgear cubicles. This is much smaller than other FLCB designs seen to date, and further size reductions may be possible for a commercial product. The FCS also reduces network losses, which translates to lower operating costs. The FCS is of a novel design and has not been proven for network protection purposes in service anywhere at present.

The Standard for Indoor 12kV power electronic FLCBs [11] describes the requirements that are specific to the FLCB. The Standard for Indoor 12kV, 24kV and 36kV Metal Enclosed Switchgear for Grid and Primary Substations [12] defines the overall general requirement for the switchgear and the process to achieving technical approval for use within UK Power Networks. It is also a reference standard for the standard of equipment for particular installations.

The project will trial the 2000A FLCB installed at a primary substation, in series with a transformer incomer or interconnector or in parallel with a bus coupler/tie, to prove the technology. The trial will not exceed any fault level limits however system studies will be required in the future for use of the FLCBs as BAU in scenarios where the fault capacity might be exceeded.

A detailed description of the ABB 2000A FLCB device is provided in Annex C. ABB have however made significant changes and improvements to the design since the feasibility study [5] in July 2016. Supplementary diagrams made available at the HAZID workshop are also provided in Annex C.

3.3 TRIAL

As explained in Section 2, a FLCB's final intended BAU usage is to release fault level capacity beyond the rating of existing switchgear. However, for the purposes of the proposed trial, the fault rating limit of the existing switchgear will not be exceeded. Therefore the impact of the FLCB failing to operate on demand is similar to that of a conventional CB failure.

Additionally, during the trial, the site`s fault clearance capabilities will not be compromised as the FLCB will not be fully relied on to isolate a fault. Whenever a fault occurs during the trial, the FLCB operation (or lack of operation) is not critical for the network, as the conventional protection will take on the majority of burden for the fault clearance. The purpose of the trial is to monitor and record the FLCB performance to provide the proof for the manufacturer's claims. Based on that proof, the future use of the FLCB as BAU, where the FLCB will be relied on for fault clearance, will be decided.

For the purposes of the trial, the FLCB will be installed with two conventional CBs in series, one on either side. This design will provide the necessary back up fault current breaking requirements as well as isolation capabilities due to the nature of adding novel equipment to the network. The existence of the adjacent CBs presents the opportunity to use a modified "CB Fail" protection philosophy as an additional safety measure for the duration of the trial. Two possible designs were considered as presented below. At this stage of the project, it is not decided which modification option will be used, as the Controls and Indication requirements are currently in concept design. The proposed options are:

- Modified CB Fail option 1 - Each tripping command sent to the FLCB by the fault detection unit QR6, shall also be sent to the 2 series CBs. This means that the tripping of the traditional CBs is accelerated by the fast detection of the fault and every time the FLCB has to operate for a fault, the series CBs will open.
- Modified CB Fail option 2 - The fault detection & tripping unit QR6 has an internal supervision feature. If there is an internal relay fault, this information can be sent to the adjacent CBs protection relays by a signalling contact. The protection relays can then take appropriate measures depending on the logic configuration.

The introduction of the two modified CB Fail protection options for the trial have negligible costs and are a test precaution. They do not therefore require an implementation assessment. They are separate to the three safety measures being considered for BAU in Section 5.2.5.

To understand the main risks with the FLCB concept, and try to mitigate them as far as possible during the design and verification phase, several activities were initiated. This includes, for instance, Failure Modes and Effects Analysis (FMEA), network simulations, PFD reliability analysis and various verification activities. Some of the more critical functions are mentioned below and are addressed in the design and verification activities planned within the project.

- Endurance of the FCS
- Interruptions capability of the Bi-mode Insulated Gate Transistor (BiGT's)
- Commutation capability of the FCS
- Insulation withstand of the FCS

- Short circuit capability of the FCS
- Failures with possible arcing in the panel
- Effect of single components on the overall reliability
- Reliability of the FCS drive circuit
- Reliability of FLCB controller

Section 5.3.3 provides reference to the evidence of the verification activities and standardised testing that support the argument that the FLCB device has been tested and commissioned for use at the specified trial site.

4. SAFETY CASE PROCESS AND PRINCIPLES

4.1 SAFETY MANAGEMENT PROCESS

A Safety Case Process and Principles document [9] has been produced 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. An overview of the safety management process is shown in Figure 1. Details of how each step in the process has been used to develop the safety argument can be found in Section 5 of this Preliminary Safety Case Report (PSCR).

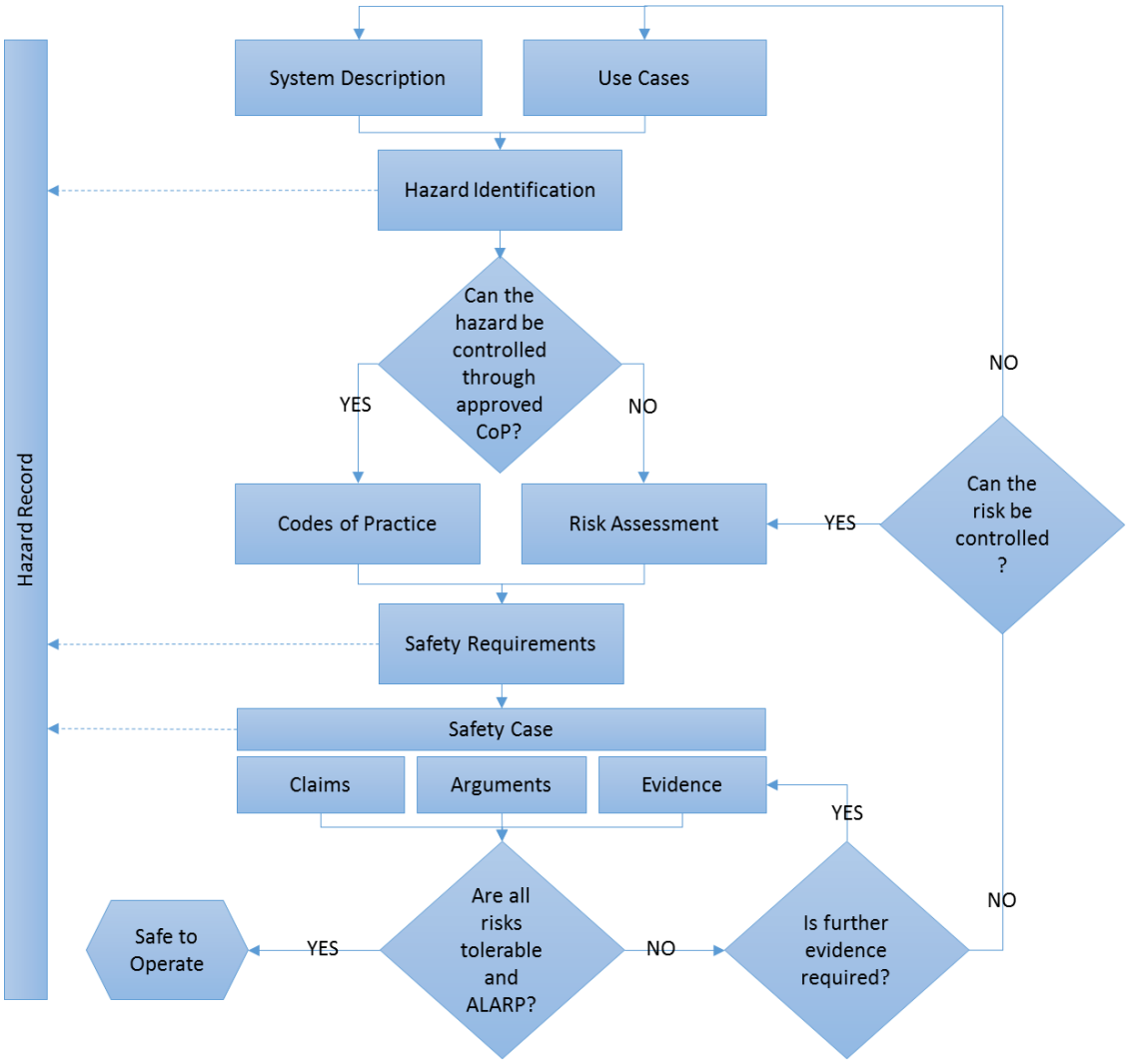


Figure 1: Safety Management Process

4.2 SAFETY CASE PRINCIPLES

The following high level safety case principles (SCPs) have been derived which have informed the case development process.

SCP 1 The Safety Case should demonstrate that the management system (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 of 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.

4.3 ACCEPTANCE CRITERIA

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. The Safety Case presents the safety argument to support the following 'Top Goal':

"The FLCB device and any required safety control shall be sufficiently reliable, or have suitable mitigation installed, such that the safety risks associated with the network equipment seeing a fault current above its rating is 'Broadly Acceptable' or that the risk has been reduced to be 'Tolerable and ALARP'.

5. SAFETY CLAIMS, ARGUMENTS AND EVIDENCE

5.1 OVERVIEW

The overall safety argument for the FLCB device is expressed using a “Claims, Argument and Evidence” (CAE) structure. 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, will result in the FLCB device having an acceptable level of safety. 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. The status of each piece of evidence is defined as:

- Green – A complete issued version of the evidence is held;
- Yellow – A draft version or a reference to the evidence is held; and
- Orange – No evidence currently exists.

The CAE approach allows the safety argument to be presented pictorially which shows the links between each piece of *evidence*, *argumen*t and *claim* that it supports. Figure 2 below provides a definition for each aspect and detail on how the diagram is presented.

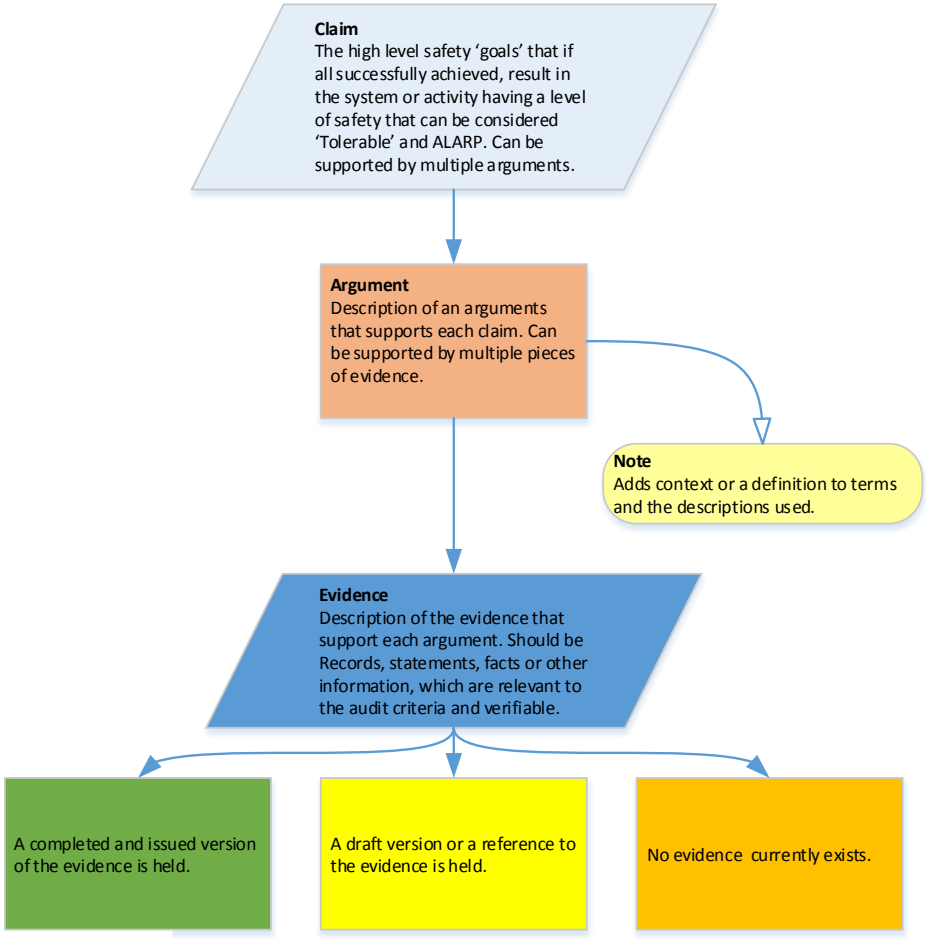


Figure 2: CAE Definition Diagram

The CAE diagram for the FLCB device can be found in Annex A.1 which identifies four key safety *claims (C1, C2, C3 and C4)* all supporting the overall "Top Goal".

The following sections present each safety claim, associated arguments and the evidence that supports it. Each piece of evidence can be found in the Safety Case Evidence Table in Annex B along with the associated reference and evidence status.

5.2 CLAIM C1 – SAFETY REQUIREMENTS

"A suitable and sufficient safety assessment process has been undertaken and appropriate Safety Requirements have been derived."

The Safety Management process is defined in the Safety Case Process and Principles document [9] and is summarised in Section 4.1 of this Report. This Section details how each individual step is used to produce the safety case for the FLCB device.

5.2.1 Argument (C1A1)

"The FLCB device and its use case has explicitly been defined and described."

In order to bound the scope of the Safety Case it is important to explicitly define and describe the ABB FLCB device and its use case. This ensures that the activities undertaken to develop the Safety Case are well focussed and provide credible evidence to the process.

A detailed description of the ABB FLCB Device can be found in Annex C of this Report.

Evidence (C1A1E1)

"Technical specifications have been produced which set out the requirements for the device and systems related to the Powerful-CB project."

The Standard for Indoor 12kV Power-Electronic FLCBs [E21] sets out the requirements for indoor FLCBs being trialled as part of the Powerful-CB project.

The Standard for Indoor 12kV, 24kV and 36kV Metal Enclosed Switchgear for Grid and Primary Substations [E22] sets out the requirements for indoor switchgear at these substations for UKPN.

Evidence (C1A1E2)

"*An Implementation as input to safety case study for the device has been produced by ABB"*

The Implementation *as input to safety case study* [E8] for the ABB FLCB Device contains a concept description, panel integration, network configuration and control system implementation and interaction overview for the FLCB device.

5.2.2 Argument (C1A2)

"A systematic approach has been used to identify all reasonably foreseeable hazards that apply to the 'system' together with potential initiating events or sequences of events."

The purpose of the Hazard Identification (HAZID) undertaken is to identify all reasonably foreseeable hazards which are then assessed. The HAZID should be systematic and structured. Correct HAZID underpins the whole risk management process and gives assurance that the risks will be managed in the project.

During the feasibility study Preliminary Hazard Identification (PHI) was undertaken to help the gain an understanding of the bounding challenge to safety that the FLCB is designed to provide protection against. The PHI also helped to identify whether the device might introduce any other undesirable consequences that have a detrimental impact on safety.

Following on from the feasibility study a HAZID Workshop was held on 21st June 2017 at the Frazer-Nash offices in Dorking. The workshop was conducted using a 'guide word examination' technique which is a deliberate search for deviations from the design intent. Attendees were asked to apply a series of 'Guidewords' in conjunction with 'Parameters' to each 'Node' to generate deviations from the design intent which can lead to undesirable consequences.

This HAZID workshop was chaired and staffed by Suitably Qualified and Experienced (SQEP) persons, and a record of their relevant qualifications and experience kept. Prior to commencement of the workshop, the team present was assessed by the HAZID Chairman to confirm they are SQEP.

Evidence (C1A2E1)

"A Preliminary hazard identification has been carried out to support the safety case feasibility assessment."

The Feasibility of Safety Case Report [E4] includes a summary of the approach taken and the results and conclusions drawn from the information. It consisted of three stages:

- Identifying the bounding safety challenge;
- Failure mode identification; and
- Hazard identification.

Evidence (C1A2E2)

"A HAZID workshop was undertaken to identify hazards for the FLCB device in both trials and general application."

The full output of the workshop is contained within the HAZID Workshop Report [E2].

The HAZID workshop was preceded by a Briefing Note [E1] which described the system and scope to be considered and the methodology being proposed for use in that workshop.

The hazards and all accompanying information identified during the workshop have been used to create the project Hazard Record [E3].

Evidence (C1A2E3)

"The HAZID was carried out by SQEP individuals."

An attendance sheet is shown in the HAZID Workshop Report [E2] and signed SQEP forms for each attendee are held separately on record by Frazer-Nash.

5.2.3 Argument (C1A3)

"Methodology and evaluation criteria adopted for the risk assessment is clear and has been developed specifically for the use of ABB FLCB devices on the electricity distribution network"

For assessment of risk for the use of the ABB FLCB device on the electricity distribution network a risk classification matrix is used which defines the boundaries between the 'Unacceptable', 'Tolerable' and 'Broadly Acceptable' regions for both the exposed worker (staff or contractors) and the general public.

The risk matrix has been developed specifically for use of the FLCB device on the electricity distribution network. This is based on the Health and Safety Executive (HSE) upper limit of tolerability for individual risk per annum for workers and for members of the public and calibrated specifically to the risk associated with the FLCB, accounting for the specific hazards and exposure size in question.

Evidence (C1A3E1)

"The risk classification matrix and acceptance criteria are documented and communicated to relevant stakeholders"

The risk classification matrix, including details of its derivation, are detailed in the Safety Case Process and Principles Document [E5].

Consequences used in the risk classification matrices relate to personal injury, property damage and environmental impact are taken from UKPN Incident Reporting Procedure [E18].

5.2.4 Argument (C1A4)

"A suitably sufficient and robust process has been undertaken to evaluate and assess safety risks and identify reasonably practicable Safety Measures"

The Risk Assessment followed on from the HAZID activities as an essential part of the hazard management process in order to assess whether the risks arising from use of the two FLCB devices on the 11kV network can be controlled to levels which are Tolerable and ALARP.

Three main consequences were identified, these are:

- Network exposed to excessive fault current;
- Flashover / local explosion; and
- Electric shock.

The Risk Assessment (RA) workshop, held on the 27th September 2017, focused on assessing the consequences and any secondary consequences which may follow. Each consequence was assessed to determine the exposure group, severity in terms of harm, asset damage and environmental damage and the likelihood of occurrence.

The workshop then identified any other potential Safety Measures that could be implemented to reduce the risk to a level that is tolerable and ALARP.

The RA workshop was chaired and staffed by SQEP persons, and a record of their relevant qualifications and experience kept. Prior to commencement of the workshop, the team present was assessed by the Workshop Chairman to confirm they are SQEP.

It was determined that the likelihood of flashover following installation of the FLCB devices or an electric shock from the FLCB device is no different from any other type of switchgear. The same controls apply based on switchgear construction standards, relevant good practice of current switchgear and following current procedures. As such these safety risks can be considered to be 'Broadly Acceptable'.

However, it was recognised that a disruptive failure of a circuit breaker due to the network being exposed to excessive fault current would pose a risk that is different to what is currently present. This risk was therefore agreed to be investigated further using a CBA.

Evidence (C1A4E1)

"A Risk Assessment workshop was undertaken to assess risks of implementing the FLCB device on the network and to identify potential Safety Measures"

The full output of the workshop is contained within the RA Workshop Report Issue 1 [E6].

The RA workshop was preceded by a Briefing Note [E7] which described the system and scope to be considered and the methodology being proposed for use in that workshop.

The Safety Measures and all accompanying information identified during the workshop have been used to create the project Hazard Record [E3].

Evidence (C1A4E2)

"RA Workshop was carried out by SQEP individuals."

An attendance sheet is shown in the RA Workshop Report Issue 1 [E6] and signed SQEP forms for each attendee are held separately on record by Frazer-Nash.

5.2.5 Argument (C1A5)

"*Cost Benefit Analysis has been carried out, using recognised methodologies and robust data, to determine whether potential Safety Measures are necessary to ensure safety so far as is reasonably practicable."*

CBA can be used as part of ALARP decisions and aids the decision making process by giving monetary values to the costs and benefits, including safety benefits, of various options. This enables a comparison of the advantages and disadvantages of multiple options to be compared using the 'like quantity' of financial value.

The CBA is based on findings from the RA workshop held on the 27th September 2017. It evaluates the safety mitigations identified at the Workshop and uses data sourced from multiple Actions raised at the Workshop.

The CBA determines whether the cost to implement the additional Safety Measures identified in the RA workshop is grossly disproportionate to the safety benefit obtained. This informs the ALARP decision for the risk of a 'disruptive failure of circuit breaker'.

Three Safety Measures were agreed to be included in the analysis, these are:

- Option 1 – Adaptive Protection;
- Option 2 – CB Fail Approach; and
- Option 3 – Ultra-Fast Earth Switch.

Determination of the risk benefit offered by each of the above Safety Measures has been considered in isolation by comparison to the baseline risk (i.e. the unmitigated risk associated with 'disruptive failure to a circuit breaker'), in order to determine the ALARP solution.

Evidence (C1A5E1)

"The input data used in the CBA is accurate and relevant"

The data used for the CBA is listed in Appendix C of the RA workshop Report Issue 2 [E19] each supplemented with a reference.

Evidence (C1A5E2)

"The CBA was conducted in accordance with recommended good practice"

The RA workshop Report Issue 2 [E19] summarises the outputs of the RA Workshop and details the findings of the CBA. It contains an analysis of the three identified Safety Measures and comparison against the existing network and baseline option. Sensitivity analysis was used to ensure suitably cautious assumptions have been made and allows the robustness of the outcomes of the CBA to be assessed.

The Safety Measures and all accompanying information identified during the workshop are detailed in the project Hazard Record [E3].

5.2.6 Argument (C1A6)

"Safety requirements have been derived from relevant applicable policies, procedures or regulations and the Risk Assessment."

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 and assessed. Where relevant, control measures identified by the hazard management process are designated as Safety Requirements. Safety requirements have also been derived from the relevant applicable policies, procedures or regulations.

Hazards may also be suitably controlled though the application of UKPN policies and procedures or by adherence to Regulations. Where this is identified as being the case no further risk assessment was undertaken. Where these risks were not covered, Safety Requirements were formed from the RA and CBA.

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 the device. Safety requirements and evidence of compliance against them is held within the Hazard Record.

Evidence (C1A6E1)

"*A HAZID workshop was undertaken which derived the Safety Requirements."*

The full output of the workshop is contained within the HAZID Workshop Report [E2].

Evidence (C1A6E2)

"A Risk Assessment workshop and CBA was undertaken which derived Safety Requirements."

The full output of the workshop and subsequent CBA is contained within the RA Workshop Report Issue 2 [E19].

Evidence (C1A6E3)

"*A Hazard Record has been developed which details the Safety Requirements*."

A Hazard Record [E3] has been produced for the ABB device to capture the output from HAZID and RA activities. The Hazard Record is a live document and is continually updated throughout the project.

5.2.7 Argument (*C1A7*)

"The outputs from all safety related activities are recorded and continually updated throughout the project"

The Hazard Record will remain live and continue to be managed throughout the project. It records the outputs from the HAZID activities, RA and Safety Measures / Safety Requirements. Following this it will be used to track the project progress against the following:

- Actions raised at the various safety related activities that may be used to form a Safety Requirement.
- Compliance with relevant policies, procedures or regulations.
- Safety requirements by referencing evidence demonstrating that they have been implemented.

Evidence (C1A7E1)

"*A Hazard Record has been developed and is continually updated throughout the project*."

A Hazard Record [E3] has been produced for the ABB device to capture the output from HAZID and RA activities. The Hazard Record is a live document and is continually updated throughout the project.

5.3 CLAIM C2 – FLCB DESIGN

"The FLCB device is designed to operate effectively and safely for all postulated network fault conditions and satisfies the derived Safety Requirements."

Supporting information around the design of the FLCB device can be found in Annex A of this report. This Section details the activities associated with the development process of the design of the FLCB device so to meet the Safety Requirements.

5.3.1 Argument (C2A1)

"The FLCB device has been designed by competent designers to operate effectively and correctly."

The FLCB device has been designed to operate satisfactorily for the system parameters and meets the various design requirements set out in the applicable standards.

Due to the nature of the device and the environment that it will be used in safety has been considered through all stages of the project. Principles such as 'Diversity' and 'Redundancy' have been considered when designing the device and the system so to enhance the integrity and reliability of safety systems.

Evidence (C2A1E1)

"*Internal UKPN Standards have been followed to ensure the device and associated equipment to be installed at the Grid and Primary substations operate effectively and correctly."*

The standard for Indoor 12kV Power-Electronic FLCBs [E21] lists a number requirements for the design and construction of the FLCB device. The standard for Indoor 12kV, 24kV and 36kV Metal Enclosed Switchgear for Grid and Primary Substations [E22] lists additional design requirements and requirements for the maintenance and operation of the device. This equipment shall be designed to meet the normal service conditions for indoor switchgear and controlgear as specified in clause 2.2 of ENA TS 41-36.

Evidence (C2A1E2)

"ABB FLCB Implementation as input to safety case study"

The Implementation *as input to safety case study* [E8] provides details of Powerful-CB project members and responsibilities. The report details the various safety activities and verification activities undertaken prior to the trial for it to work effectively and correctly.

5.3.2 Argument (C2A2)

"The designers have been integral to the safety assessment process and able to influence the design during the development."

The project has undertaken a series of safety assessment activities using a wide range of design expertise throughout. This has ensured the design of the device controls the risks associated and complies with relevant statutory provisions.

It is important to note that an integrated, safety-led approach has been adopted to the development of the design, and that the design development can be iterative. Reasons that a number of iterations may be required include, but are not limited to:

- Changes to the functional requirements or Safety Requirements;
- The discovery challenges to the design in the HAZID;
- The results of testing and validation; and
- The results of trials and substantiation.

Evidence (C2A2E1)

"Designers had involvement in producing a Feasibility of Safety Case Report for the ABB device"

The Feasibility Report [E4] documents the achievability of producing a safety case supporting the Powerful-CB approach: deployment of the FLCB on 11kV networks to facilitate the additional connection of Distributed Generation.

Evidence (C2A2E2)

"Designers have attended the HAZID and RA Workshops and had opportunities to review of the outputs"

The full output of the workshop is contained within the HAZID Workshop Report [E2].

The RA workshop Report Issue 2 [E19] summarises the outputs of the RA Workshop and details the findings of the CBA. It contains an analysis of the three identified potential Safety Measures and comparison against the existing network and baseline option.

Each workshop has had the SQEP personnel available to produce the required outputs. ABB have attended both the HAZID Workshop held on the 21st June 2017 and the RA Workshop held on the 27th September 2017. ABB have had consistent communication with the project and have been responsible for numerous actions raised at the workshops.

5.3.3 Argument (C2A3)

"The FLCB device has been tested and commissioned for use at the specified trial site"

Before proceeding with trials, the following activities ensure that it is safe to do so. Activities at this stage include:

- Confirm that the FLCB has been successfully built in accordance with the detailed design;
- Specify the testing required to confirm the functionality and safe operation of the FLCB;
- Establish any limitations of use for the trial period;
- Identify situations that involve personnel working on sites or in conditions that they are not familiar with;
- Review the HAZOP, FMEA and PFD reliability analysis as applicable to check this is all still relevant and correct.

At this point, substantiation of the Safety Requirements related to the device performance have not been achieved: evidence from the trial period will be key in doing so. However, there is sufficient evidence from the previous testing and validation stages to ensure that the FLCB device can be safely implemented on the network, and that the risks associated with installation

and commissioning are ALARP. This forms the basis of the installation and commissioning safety arguments in the in-service safety case.

This stage may recommend further testing or analysis before the device is considered safe to put on the network. Although less likely as the process develops, it may also identify further design changes.

Evidence (C2A3E1)

"Testing and commissioning of the FLCB device has been completed to ensure it meets its functional and safety requirements"

Verification Activities including FCS Endurance Testing, BiGT Verification Testing, BiGT Limit Testing and FLCB Endurance Testing are planned for the device. Standardised Testing will be undertaken upon finalising the design of the FLCB. This will include Interruption Testing, Temperature Rise Test, Insulation Test, Short Circuit Capability and Internal Arc Testing. Details of the Verification Activities and standardised testing of the FLCB Device can be found in the Implementation *as input to safety case study* [E8].

Evidence for the Testing and Commissioning of the ABB FLCB device can be found in document [E9].

5.3.4 Argument (C2A4)

"The FLCB device meets the legislative Safety Requirements"

Relevant legislation has derived a number of Safety Requirements for the FLCB device. Some hazards are suitably controlled through the application of UKPN policies and procedures (e.g. application of distribution safety rules) or adherence to Regulations (e.g. compliance with Electricity at Work Regulations). Where it has been identified that the device meets these requirements no further risk assessment was undertaken and compliance is recorded in the Hazard Record.

Evidence (C2A4E1)

"Legislative compliance statements have been authored"

A Hazard Record [E3] has been produced for the ABB device which includes the relevant policies and procedures regulations. The Hazard Record is a live document and is continually updated throughout the project.

5.3.5 Argument (C2A5)

"The design of the FLCB device satisfies the derived Safety Requirements"

In order to demonstrate that the 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 have been identified. Where relevant, control measures identified by the hazard management process have been designated as Safety Requirements. Compliance against these requirements is a key part of the evidence needed to build the safety case and therefore form part of the basis of the acceptance criteria for the laboratory and field trials for the device.

Safety requirements for the FLCB device ensure it performs in a safe manner when installed on the trial network or as BAU. Safety activities such as the FMEA and reliability assessments prove compliance against the derived Safety Requirements.

Evidence (C2A5E1)

"The FLCB device meets the derived Safety Requirements"

One of the key parameters in the safety and reliability considerations is the Probability of Failure on Demand, meaning the probability of the device failing to perform its safety function at a given command. The required PFD that needs to be achieved or exceeded is a Safety Requirement derived from the risk assessment. The estimation of the achieved PFD for the device is done by considering existing performance data (where available) together with test results from verification testing during the design and verification phase. It is assumed that the PFD is mainly determined by the key components: FCS; BiGT; and surge arresters. The rest of the components will need to be selected and architected in such a way that the contribution is negligible in comparison to the key components. In the design of the FLCB a modular concept is used aiming at having a safe interruption using three series connected modules. If the key components each have a probability of failure of the order of 1 per 1000 demands, and all of them need to operate properly to have overall safe operation, the device PFD would typically be $3x10^{-3}$.

The reliability data and FMEA document [E20] prove that the device's performance and the system it is to be installed upon meet the derived Safety Requirements and is safe for installation on the trial and as BAU.

A Hazard Record [E3] has been produced for the ABB device which lists each Safety Requirements against its relevant risk. It is provides a reference to the evidence for compliance against each Safety Requirements.

5.3.6 Argument (C2A6)

"The Data gathered during the trials will further substantiate the Safety Case"

Not all data is known about the performance of the ABB FLCB device and hence before the device is installed to be used as BAU a trial is being carried out. This trial will provide sets of performance data which will be used to determine whether the device will operate reliably and safely as required for BAU.

Evidence (C2A6E1)

"Trial Reports for the ABB FLCB Device"

The Trials are still to be undertaken and a report [E10] will be produced once completed.

5.4 CLAIM C3 – IMPLEMENTATION

"The ABB FLCB devices can be implemented safely onto the electricity networks"

Sufficient evidence is needed from the safety assessment process to ensure that the FLCB device can be safely implemented onto the network in line with the Commission Implementing Regulations [10]. This Section presents the various arguments and evidence that ensure the device is considered safe to put on the network in the trials.

5.4.1 *Argument* (*C3A1*)

"*A safe installation strategy has been developed for the trial"*

The purpose of the installation strategy is to offer a safe, efficient and structured approach to installing the FLCB devices onto the electricity network.

It is important to note that an integrated, safety-led approach has been adopted to the development of the system design, and that the design development can be iterative. Reasons that a number of iterations may be required include, but are not limited to:

- Changes to the functional requirements or Safety Requirements;
- The discovery challenges to the design in the hazard identification;

- The results of testing and validation; and
- The results of trials and substantiation.

Evidence (C3A1E1)

"Installation Strategy Report has been produced for the FLCB device."

The full installation strategy is contained within the Installation Strategy Report [E11].

5.4.2 Argument (C3A2)

"The commissioning activities verify that the FLCB devices have been installed in accordance with the strategy."

Following installation of the devices onto the network the commissioning activities will verify that the as installed device is in accordance with the strategy and therefore meets the requirements for safe operation.

Evidence (C3A2E1)

"Installation and Commissioning Report has been produced."

The full Installation and Commissioning procedure and outputs are contained within the Installation and Commissioning Report [E12].

5.4.3 Argument (C3A3)

"Specific precautions are in place for the trial of the FLCB device on the electricity network."

Due to the nature of the device, specific precautions are in place to allow for safe operation. As such the potential fault current limit of the network at present will not be exceeded. However, it is important that the full FLCB capability needs to be extensively tested in a representative scenario to gain confidence in its operation for its use in BAU application i.e. with increased fault current levels.

Evidence (C3A3E1)

"A Trial Installation Strategy Report has been produced."

The full installation strategy is contained within the Installation Strategy Report [E11].

5.4.4 Argument (C3A4)

"There is sufficient resources to support the implementation of the FLCB Device for the trial and BAU."

The trial will require extra workforce and an analysis team, however it should not be done in a way that creates an un-realistic environment that is unsustainable during BAU.

Evidence (C3A4E1)

"Resource plan for the implementation of the FLCB device for both the Trial and BAU has been produced."

A plan [E13] identifying the required workforce and resources for the trial of the ABB device has been produced.

5.5 CLAIM C4 - OPERATION

"The safe operation of the FLCBs can be sustained throughout the trial, the workforce is capable of delivering and assuring what is expected and they are supported by accurate asset information."

It is necessary that the risks of the FLCB device in normal operation do not introduce any unexpected or additional safety risks. This Section presents the arguments and evidence to support the safe operation of the FLCB device on the network.

5.5.1 Argument (C4A1)

"The workforce is trained and competent to discharge their duties."

Implementation of the devices onto the network for both the trial and BAU will require trained and competent personnel. This is to ensure a safe installation and that the devices operate as intended which will reduce risks in future operations.

Evidence (C4A1E1)

"Training schedule and documents have been produced and competence management framework is in place to deliver a capable workforce."

Details of the training, specific training documents and the competence framework can be found in the Training and Competence Plan [E14].

5.5.2 Argument (C4A2)

"Sufficient and appropriate resources are available to enable the workforce to discharge their duties."

For safe and efficient operation trained and competent personnel must be available for the required tasks for BAU.

Evidence (C4A2E1)

"A Resource plan has been produced to ensure resource needs requirements and appropriate tools are in place and available when required."

A Resource Plan [E13] identifying the required workforce and resources for the trial of the ABB device has been produced.

5.5.3 Argument (C4A3)

"A fit for purpose assurance management system exists."

For safe installation, maintenance and operation an assurance management system must be in place.

Evidence (C4A3E1)

"Contractors operate robust assurance regimes that monitor and assess the performance of the FLCB devices."

The Assurance Management System document [E15] contains the details of the robust assurance regimes that contractors adhere to.

5.5.4 Argument (C4A4)

"The state of the infrastructure at any point in time is defined and available."

For safe installation, maintenance and operation the state of the infrastructure must be known.

Evidence (C4A4E1)

"Infrastructure Reports are produced and include any planned changes"

Details of the status and any planned changes to infrastructure are contained within the Infrastructure Reports [E16].

5.6 EVIDENCE SUMMARY

Annex B of this report lists each piece of evidence which is used to support the augments and claims made in Section 5.

Claim 1 contains arguments supporting the safety assessment of the device. Various safety activities undertaken as part of the project and supporting documents support this claim. The documents provide clear and concise arguments as listed in Section 5.2.

Claim 2 is supported by arguments which prove the device meets the Safety Requirements. The reliability of the device is based on predicted data, which is less robust than trials data, and hence the need for the trials before implementing the devices on the network for BAU. The trials will then substantiate the Safety Requirements derived from the predicted data. Evidence currently missing to support this claim include a Reliability Data and FMEA Document and a Trial Report for the Device. The first two will be produced prior to the commencement of the trials and the third following the completion of the trials.

Claim 3 is supported by arguments detailing how the devices will be installed onto the network. Large evidence gaps still exist involving plans, schedules and strategies detailing how this will be completed. It considers this for both the trial and for BAU and includes an Installations Strategy, Installation and Commissioning Report and a Resource Plan for the trial. These evidence documents will be produced prior to installation works for the trial.

Claim 4 relates to the safe operation and maintenance of the devices. Evidence still to be provided to support this claim include a Training and Competence Plan, an Assurance Management System Document and an Infrastructure Report. These evidence documents will be produced after the completion of the trials.

6. CONCLUSIONS

The safety activities undertaken as part of this process have supported a safety-led approach to the development of the system design and the safety case.

Following HAZID and RA Workshops, the likelihood of either a Flashover / Local Explosion or Electric Shock as a result of a fault with the FLCB device was agreed to be no different to any other type of switchgear that is currently installed on the network. Therefore the risk is no different and should be considered 'Broadly Acceptable' on this basis.

However, outside the trial, the consequence of the network being exposed to excessive fault current could lead to the disruptive failure of a circuit breaker and potentially result in an explosion within the sub-station and lead to a fire with an oil circuit breaker present. A risk assessment was undertaken to assess the tolerability of this risk and a CBA was undertaken on various potential Safety Measures to support a decision as to whether these risks are ALARP. The analysis concluded that, due to the high reliability of the devices, the safety risk is tolerably low and the cost to implement any of the three potential Safety Measure options is grossly disproportionate to the safety benefit gained.

The high reliability of the device is therefore crucial to the validity of this analysis and thus the safety case. A key Safety Requirement was therefore derived from the CBA for the PFD of the ABB device to be less than $1x10^{-3}$. The certification of the design of the device proving the reliability is a key part of the evidence and is used to support the claim that "the FLCB device is designed to operate effectively and safely for all postulated network fault conditions and satisfies the derived Safety Requirements" (Claim C2).

During the trials the potential fault current limit of the network will not be exceeded, therefore the potential safety measures identified at the RA workshop to mitigate this are not required. In addition, the FLCB will have adjacent conventional circuit breakers. Therefore the risk can be considered to be no worse than existing operations and the protection is beyond that used in the usual design scope.

However, it is important that the full FLCB capability needs to be extensively tested in a representative scenario to gain confidence in its operation for its use in BAU application i.e. with increased fault current levels.

The results of the trial will also further influence the design and development of maintenance schedules and operator instructions. These will be used to revalidate and update elements of the safety case prior to extended operations and ultimately commercial operation.

In summary this PSCR concludes that:

1. The hazards associated with the FLCB device are understood and sufficiently managed such that the operation and implementation of the device at the trials site can be considered to be 'Safe', whereby the risks have been reduced to a level that is either 'Broadly Acceptable' or 'Tolerable and ALARP'.
2. Provided that the reliability of the FLCB device can be proven during the trial period, and that the risks associated with construction / installation are understood and will be adequately controlled, a suitable 'case for safety' can be made for operation of the FLCB device in BAU application such that the safety risks associated with the network equipment seeing a fault current above its rating can be 'Broadly Acceptable' or that the risk can be reduced to be 'Tolerable' and 'ALARP'.

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] FNC 50235/44699R Feasibility of safety case for ABB hybrid fault current limiter, 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] HSE, 2001, Reducing Risks, Protecting People, HSE's decision-making process.

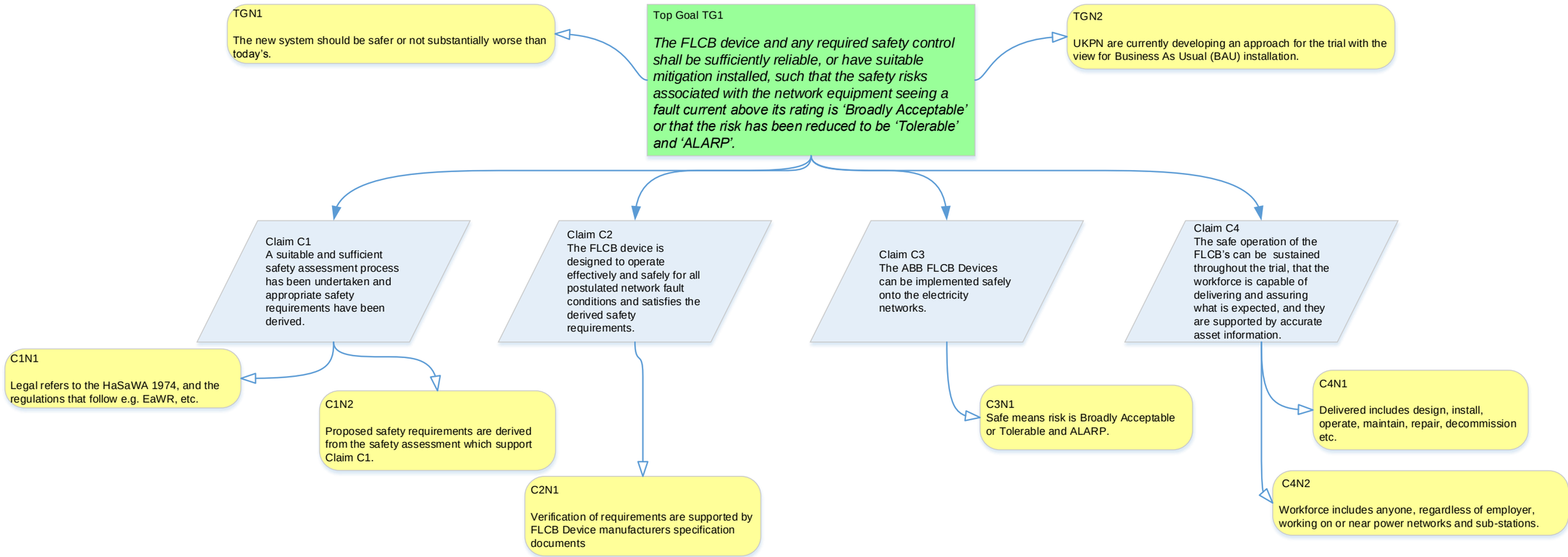
[9] FNC 52680-45804R, Powerful-CB Safety Case Process and Principles, Issue 1, 5th May 2017.

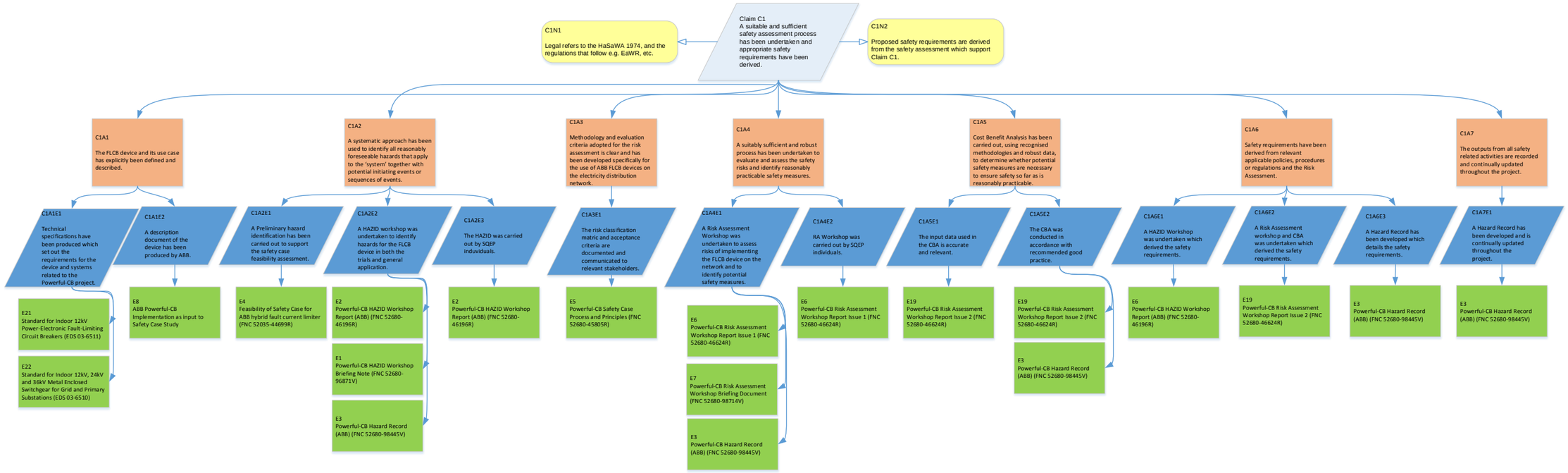
[10] Commission Implementing Regulations (EU) 2015/1136 amending Implementing Regulation (EU) No. 402/2013 on the Common Safety Method for Risk Evaluation and Assessment.

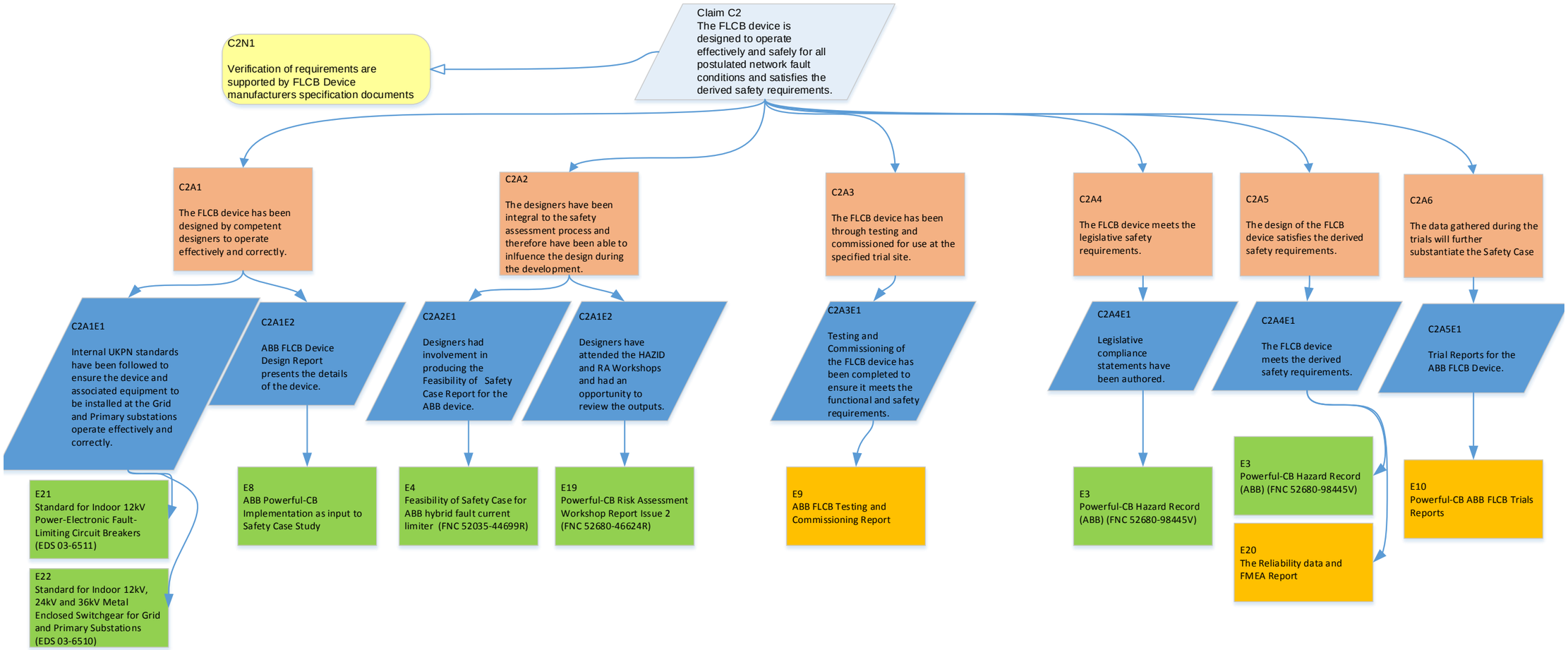
[11] ETS 03 –6511, Standard for Indoor 12kV Power-Electronic Fault-Limiting Circuit Breakers, Version 1.1, June 2017.

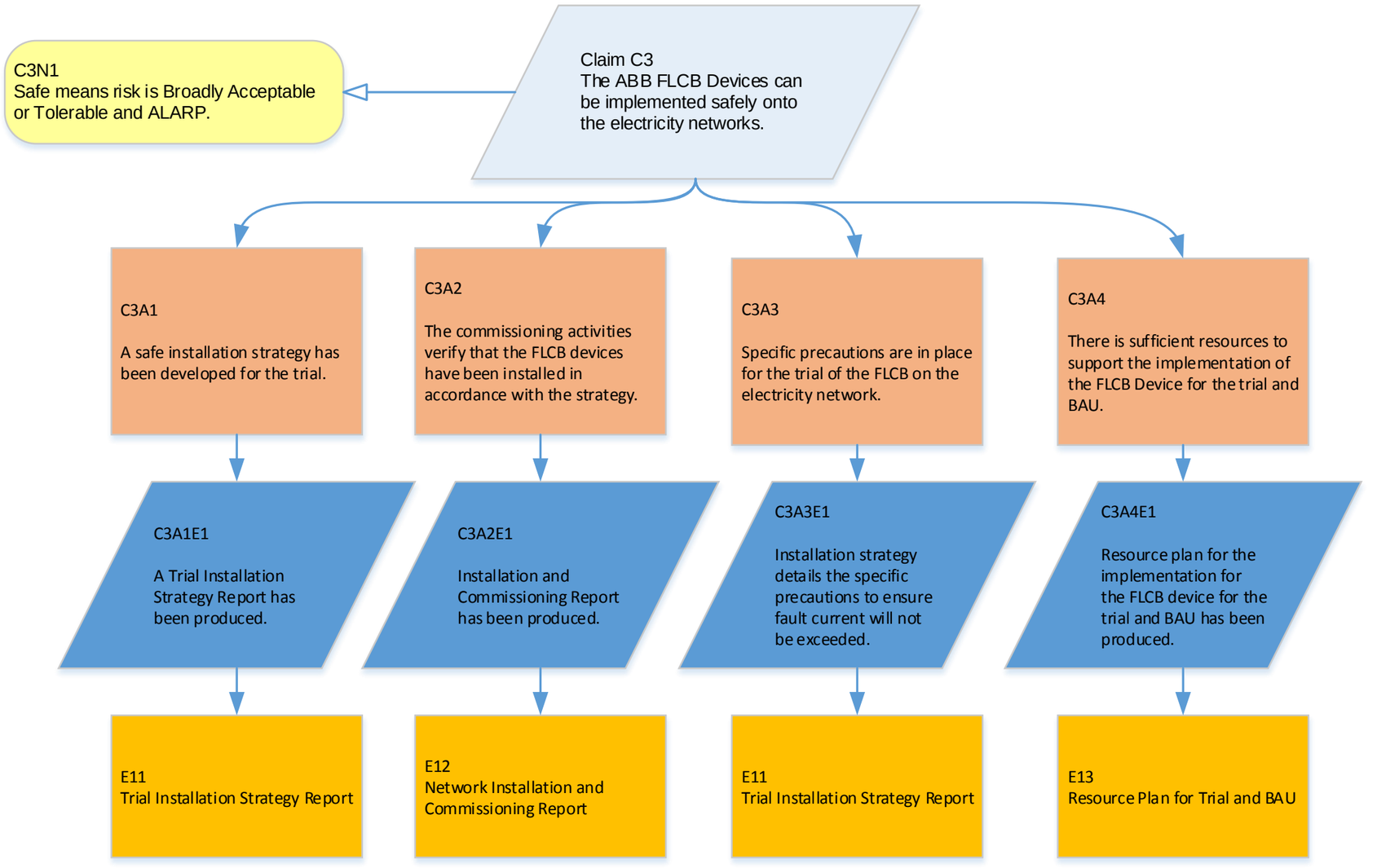
[12] ETS 03-6510, Standard for Indoor 12kV, 24kV and 36kV Metal Enclosed Switchgear for Grid and Primary Substations, Version 5.0, August 2017.

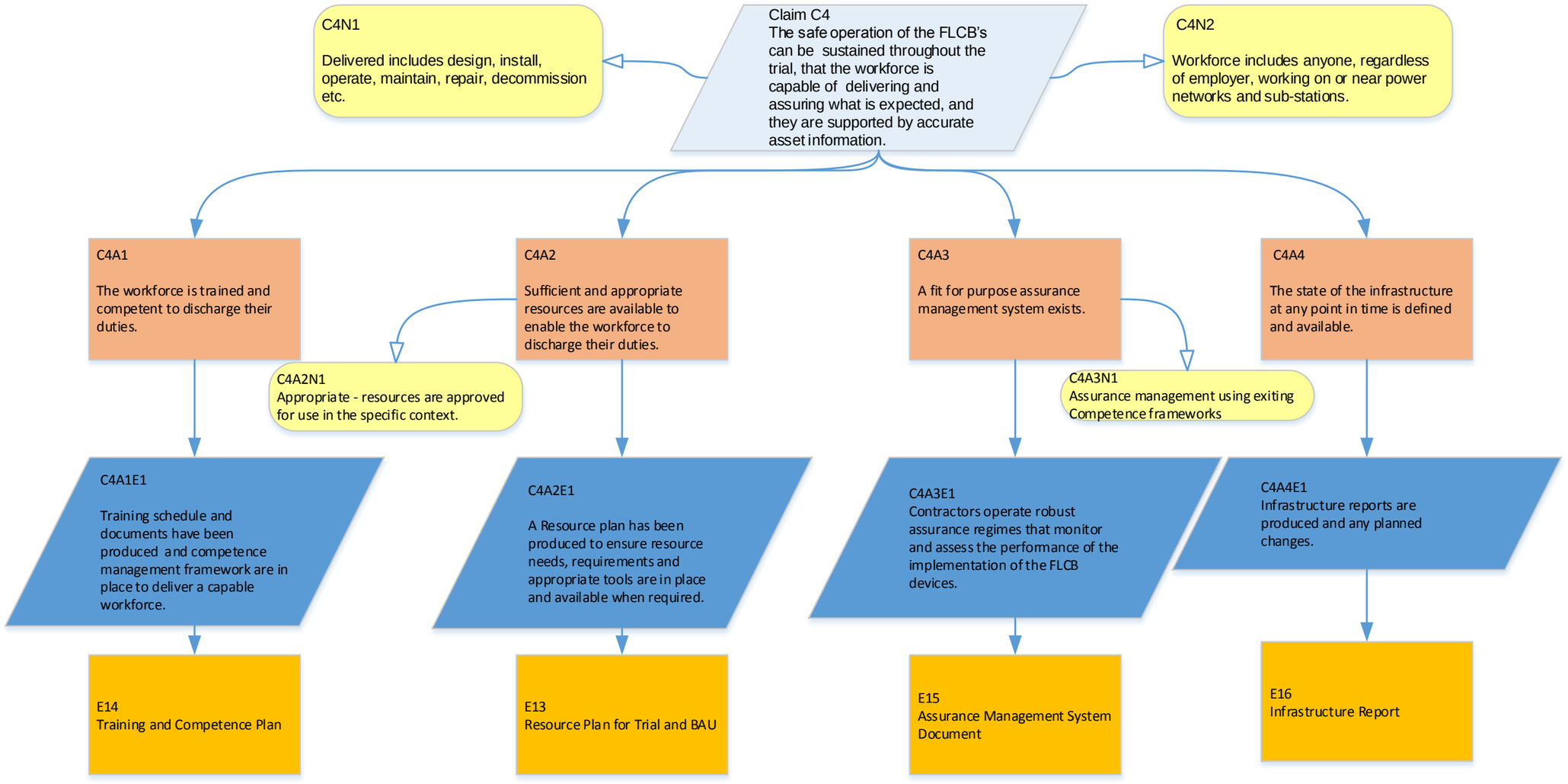
ANNEX A - CLAIMS, ARGUMENTS, EVIDENCE DIAGRAMS


TGN1
The new system should be safer or not substantially worse than today's.
Top Goal TG1
The FLCB device and any required safety control shall be sufficiently reliable, or have suitable mitigation installed, such that the safety risks associated with the network equipment seeing a fault current above its rating is 'Broadly Acceptable' or that the risk has been reduced to be 'Tolerable' and 'ALARP'.
TGN2
UKPN are currently developing an approach for the trial with the view for Business As Usual (BAU) installation.
Claim C1
A suitable and sufficient safety assessment process has been undertaken and appropriate safety requirements have been derived.
Claim C2
The FLCB device is designed to operate effectively and safely for all postulated network fault conditions and satisfies the derived safety requirements.
Claim C3
The ABB FLCB Devices can be implemented safely onto the electricity networks.
Claim C4
The safe operation of the FLCB's can be sustained throughout the trial, that the workforce is capable of delivering and assuring what is expected, and they are supported by accurate asset information.
C1N1
Legal refers to the HaSaWA 1974, and the regulations that follow e.g. EaWR, etc.
C1N2
Proposed safety requirements are derived from the safety assessment which support Claim C1.
C2N1
Verification of requirements are supported by FLCB Device manufacturers specification documents
C3N1
Safe means risk is Broadly Acceptable or Tolerable and ALARP.
C4N1
Delivered includes design, install, operate, maintain, repair, decommission etc.
C4N2
Workforce includes anyone, regardless of employer, working on or near power networks and sub-stations.


Claim C1
A suitable and sufficient safety assessment process has been undertaken and appropriate safety requirements have been derived.
C1N1
Legal refers to the HaSaWA 1974, and the regulations that follow e.g. EaWR, etc.
C1N2
Proposed safety requirements are derived from the safety assessment which support Claim C1.
C1A1
The FLCB device and its use case has explicitly been defined and described.
C1A2
A systematic approach has been used to identify all reasonably foreseeable hazards that apply to the 'system' together with potential initiating events or sequences of events.
C1A3
Methodology and evaluation criteria adopted for the risk assessment is clear and has been developed specifically for the use of ABB FLCB devices on the electricity distribution network.
C1A4
A suitably sufficient and robust process has been undertaken to evaluate and assess the safety risks and identify reasonably practicable safety measures.
C1A5
Cost Benefit Analysis has been carried out, using recognised methodologies and robust data, to determine whether potential safety measures are necessary to ensure safety so far as is reasonably practicable.
C1A6
Safety requirements have been derived from relevant applicable policies, procedures or regulations and the Risk Assessment.
C1A7
The outputs from all safety related activities are recorded and continually updated throughout the project.
C1A1E1
Technical specifications have been produced which set out the requirements for the device and systems related to the Powerful-CB project.
C1A1E2
A description document of the device has been produced by ABB.
C1A2E1
A Preliminary hazard identification has been carried out to support the safety case feasibility assessment.
C1A2E2
A HAZID workshop was undertaken to identify hazards for the FLCB device in both the trials and general application.
C1A2E3
The HAZID was carried out by SQEP individuals.
C1A3E1
The risk classification matric and acceptance criteria are documented and communicated to relevant stakeholders.
C1A4E1
A Risk Assessment Workshop was undertaken to assess risks of implementing the FLCB device on the network and to identify potential safety measures.
C1A4E2
RA Workshop was carried out by SQEP individuals.
C1A5E1
The input data used in the CBA is accurate and relevant.
C1A5E2
The CBA was conducted in accordance with recommended good practice.
C1A6E1
A HAZID Workshop was undertaken which derived the safety requirements.
C1A6E2
A Risk Assessment workshop and CBA was undertaken which derived the safety requirements.
C1A6E3
A Hazard Record has been developed which details the safety requirements.
C1A7E1
A Hazard Record has been developed and is continually updated throughout the project.
E21
Standard for Indoor 12kV Power-Electronic Fault-Limiting Circuit Breakers (EDS 03-6511)
E22
Standard for Indoor 12kV, 24kV and 36kV Metal Enclosed Switchgear for Grid and Primary Substations (EDS 03-6510)
E8
ABB Powerful-CB Implementation as input to Safety Case Study
E4
Feasibility of Safety Case for ABB hybrid fault current limiter (FNC 52035-44699R)
E2
Powerful-CB HAZID Workshop Report (ABB) (FNC 52680-46196R)
E1
Powerful-CB HAZID Workshop Briefing Note (FNC 52680-96871V)
E3
Powerful-CB Hazard Record (ABB) (FNC 52680-98445V)
E2
Powerful-CB HAZID Workshop Report (ABB) (FNC 52680-46196R)
E5
Powerful-CB Safety Case Process and Principles (FNC 52680-45805R)
E6
Powerful-CB Risk Assessment Workshop Report Issue 1 (FNC 52680-46624R)
E7
Powerful-CB Risk Assessment Workshop Briefing Document (FNC 52680-98714V)
E3
Powerful-CB Hazard Record (ABB) (FNC 52680-98445V)
E6
Powerful-CB Risk Assessment Workshop Report Issue 1 (FNC 52680-46624R)
E19
Powerful-CB Risk Assessment Workshop Report Issue 2 (FNC 52680-46624R)
E19
Powerful-CB Risk Assessment Workshop Report Issue 2 (FNC 52680-46624R)
E3
Powerful-CB Hazard Record (ABB) (FNC 52680-98445V)
E6
Powerful-CB HAZID Workshop Report (ABB) (FNC 52680-46196R)
E19
Powerful-CB Risk Assessment Workshop Report Issue 2 (FNC 52680-46624R)
E3
Powerful-CB Hazard Record (ABB) (FNC 52680-98445V)
E3
Powerful-CB Hazard Record (ABB) (FNC 52680-98445V)


Claim C2
The FLCB device is designed to operate effectively and safely for all postulated network fault conditions and satisfies the derived safety requirements.
C2N1
Verification of requirements are supported by FLCB Device manufacturers specification documents
C2A1
The FLCB device has been designed by competent designers to operate effectively and correctly.
C2A2
The designers have been integral to the safety assessment process and therefore have been able to inlfuence the design during the development.
C2A3
The FLCB device has been through testing and commissioned for use at the specified trial site.
C2A4
The FLCB device meets the legislative safety requirements.
C2A5
The design of the FLCB device satisfies the derived safety requirements.
C2A6
The data gathered during the trials will further substantiate the Safety Case
C2A1E1
Internal UKPN standards have been followed to ensure the device and associated equipment to be installed at the Grid and Primary substations operate effectively and correctly.
C2A1E2
ABB FLCB Device Design Report presents the details of the device.
C2A2E1
Designers had involvement in producing the Feasibility of Safety Case Report for the ABB device.
C2A1E2
Designers have attended the HAZID and RA Workshops and had an opportunity to review the outputs.
C2A3E1
Testing and Commissioning of the FLCB device has been completed to ensure it meets the functional and safety requirements.
C2A4E1
Legislative compliance statements have been authored.
C2A4E1
The FLCB device meets the derived safety requirements.
C2A5E1
Trial Reports for the ABB FLCB Device.
E21
Standard for Indoor 12kV Power-Electronic Fault-Limiting Circuit Breakers (EDS 03-6511)
E22
Standard for Indoor 12kV, 24kV and 36kV Metal Enclosed Switchgear for Grid and Primary Substations (EDS 03-6510)
E8
ABB Powerful-CB Implementation as input to Safety Case Study
E4
Feasibility of Safety Case for ABB hybrid fault current limiter (FNC 52035-44699R)
E19
Powerful-CB Risk Assessment Workshop Report Issue 2 (FNC 52680-46624R)
E9
ABB FLCB Testing and Commissioning Report
E3
Powerful-CB Hazard Record (ABB) (FNC 52680-98445V)
E3
Powerful-CB Hazard Record (ABB) (FNC 52680-98445V)
E20
The Reliability data and FMEA Report
E10
Powerful-CB ABB FLCB Trials Reports


C3N1
Safe means risk is Broadly Acceptable or Tolerable and ALARP.
Claim C3
The ABB FLCB Devices can be implemented safely onto the electricity networks.
C3A1
A safe installation strategy has been developed for the trial.
C3A2
The commissioning activities verify that the FLCB devices have been installed in accordance with the strategy.
C3A3
Specific precautions are in place for the trial of the FLCB on the electricity network.
C3A4
There is sufficient resources to support the implementation of the FLCB Device for the trial and BAU.
C3A1E1
A Trial Installation Strategy Report has been produced.
C3A2E1
Installation and Commissioning Report has been produced.
C3A3E1
Installation strategy details the specific precautions to ensure fault current will not be exceeded.
C3A4E1
Resource plan for the implementation for the FLCB device for the trial and BAU has been produced.
E11
Trial Installation Strategy Report
E12
Network Installation and Commissioning Report
E11
Trial Installation Strategy Report
E13
Resource Plan for Trial and BAU


C4N1
Delivered includes design, install, operate, maintain, repair, decommission etc.
Claim C4
The safe operation of the FLCB's can be sustained throughout the trial, that the workforce is capable of delivering and assuring what is expected, and they are supported by accurate asset information.
C4N2
Workforce includes anyone, regardless of employer, working on or near power networks and sub-stations.
C4A1
The workforce is trained and competent to discharge their duties.
C4A2
Sufficient and appropriate resources are available to enable the workforce to discharge their duties.
C4A3
A fit for purpose assurance management system exists.
C4A4
The state of the infrastructure at any point in time is defined and available.
C4A2N1
Appropriate - resources are approved for use in the specific context.
C4A3N1
Assurance management using exiting Competence frameworks
C4A1E1
Training schedule and documents have been produced and competence management framework are in place to deliver a capable workforce.
C4A2E1
A Resource plan has been produced to ensure resource needs, requirements and appropriate tools are in place and available when required.
C4A3E1
Contractors operate robust assurance regimes that monitor and assess the performance of the implementation of the FLCB devices.
C4A4E1
Infrastructure reports are produced and any planned changes.
E14
Training and Competence Plan
E13
Resource Plan for Trial and BAU
E15
Assurance Management System Document
E16
Infrastructure Report

ANNEX B - SAFETY CASE EVIDENCE TABLE

The status of each piece of evidence is defined as:

- Green- A complete issued version of the evidence is held;
- Yellow – A draft version or a reference to the evidence is held;
- Orange – No evidence currently exists.

Table 1: Safety Case Evidence Table

ID	Reference	Document Title	Issue / Date	Status
E1	FNC 52680-96871V	Powerful-CB HAZID Workshop Briefing Note	Issue 1 June 2017	G
E2	FNC 52680-46196R	Powerful-CB HAZID Workshop Report (ABB)	Issue 1 August 2017	G
E3	FNC 52680-98445V	Powerful-CB Hazard Record (ABB)	Issue 2 April 2018	G
E4	FNC 50235-44699R	Feasibility of safety case for ABB hybrid fault current limiter	Issue 1 August 2016	G
E5	FNC 52680-45804R	Powerful-CB Safety Case Process and Principles	Issue 1 May 2017	G
E6	FNC 52680-46624R	Powerful-CB Risk Assessment Workshop Report	Issue 1 November 2017	G
E7	FNC 52680-98714V	Powerful-CB Risk Assessment Workshop Briefing Document	Issue 1 September 2017	G
E8	Non Specific	ABB Powerful CB Implementation as input to safety case study	Rev 1 Apr-18	G
E9	TBC	ABB FLCB Testing and Commissioning Report	TBC	O
E10	TBC	Powerful-CB ABB FLCB Trial Reports	TBC	O
E11	TBC	Installation Strategy Report	TBC	O
E12	TBC	Network Installation and Commissioning Report	TBC	O
E13	TBC	Resource Plan for Trial and BAU	TBC	O
E14	TBC	Training and Competence Plan	TBC	O
E15	TBC	Assurance Management System Document	TBC	O

ID	Reference	Document Title	Issue / Date	Status
E16	TBC	Infrastructure Report	TBC	O
E17	-	Not Used	-	-
E18	HSS-01-051	UKPN Incident Reporting Procedure	Version 9.0 February 2018	G
E19	FNC 52680-46624R	Powerful-CB Risk Assessment Workshop Report	Issue 2 May 2017	G
E20	TBC	Reliability Data and FMEA Report	TBC	O
E21	ETS 03-6511	Standard for Indoor 12kV Power-Electronic Fault-Limiting Circuit Breakers	Version 1.1 June 2017	G
E22	ETS 03-6510	Standard for Indoor 12kV, 24kV and 36kV Metal Enclosed Switchgear for Grid and Primary Substations	Version 5.0 August 2017	G

ANNEX C - FLCB DEVICE SPECIFICATION

Will include Section 3 of the Implementation report when formally issued.

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

Powerful-CB

Preliminary Safety Case Report- AMAT FLCB Device

FNC 52680/47045R 1

Prepared for UK Power Networks

SYSTEMS AND ENGINEERING TECHNOLOGY

DOCUMENT INFORMATION

Project : Powerful-CB

Report Title : Preliminary Safety Case Report- AMAT FLCB Device

Client : UK Power Networks

Client Ref. : 7600003478

Classification :

Report No. : FNC 52680/47045R

Issue No. : 1

Date : 14-May-2018

Compiled By : Jamie Moore

Verified By : John Stringer

Approved By : Stephen Clark

Signed :

DISTRIBUTION

Copy	Recipient	Organisation
1	Laura Daniels	UK Power Networks
2	John Moutafidis	UK Power Networks
3	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

EXECUTIVE SUMMARY

This Preliminary Safety Case Report (PSCR) presents the overall safety argument for the Applied Materials Inc (AMAT) 250A Fault Limiting Circuit Breakers (FLCB) in a 'Claims, Arguments and Evidence (CAE)' structure. Each claim is supported by multiple arguments and a set of robust evidence.

The electricity network is inherently dangerous due to the large amounts of electrical power being transported through it. Under certain conditions this power can become uncontrolled and cause damage to equipment and injury to people. In order to reduce the likelihood of such occurrences, the risks have been eliminated or controlled as far as reasonably practicable. This is underpinned by the Distribution Network Operators legal obligation to ensure the safe operation of the electricity network.

In the current state of the network, the risks associated with switchgear are well known and managed. Following Hazard Identification (HAZID) and Risk Assessment (RA) Workshops, the likelihood of damage as a result of a fault with the FLCB device was assessed against the present risk with the currently installed Circuit Breakers and it was agreed that the use of the FLCB device did not give an increased risk compared to the current network. Therefore on the basis that the risk is no different to what is already accepted on the network, it can be considered to be 'Broadly Acceptable'.

However, the application for which the FLCB is used is new and unique to the electricity network, as it allows the potential fault currents to exceed the ratings of some network equipment. This is the additional risk that is created by the FLCB project and this safety case ultimately argues whether it can be reduced to Tolerable or ALARP.

During the trials the potential fault current limit of the network will not be exceeded, therefore the potential safety measures identified at the RA workshop to mitigate this are not required. In addition, the FLCB will have adjacent conventional circuit breakers. Therefore the risk can be considered to be no worse than existing substations in operation and the protection design is beyond the current practice.

A BAU (Business As Usual) implementation of an FLCB on the network would mean that there would not be a conventional back-up circuit breaker in series with the FLCB and additionally the fault levels would be allowed to rise above the conventional switchgear's rating. Therefore in BAU, switchgear exposure to excessive fault current could lead to disruptive failure and potentially result in an explosion within the sub-station, leading to a fire if an oil circuit breaker is present. A risk assessment was undertaken to assess the tolerability of this risk and a Cost Benefit Analysis (CBA) was undertaken on various potential Safety Measures to support a decision as to whether these risks are As Low As Reasonably Practicable (ALARP) Safety Measure. The analysis concluded that, due to the high reliability of the devices, the safety risk is tolerably low and the cost to implement any of the two potential Safety Measure options is grossly disproportionate to the safety benefit gained. This will be reviewed following the trial and further system studies may be undertaken in the future for the use of FLCBs in BAU scenarios where the fault capacity might be exceeded.

The high reliability of the device is crucial to the validity of this analysis and thus the safety case. A key Safety Requirement was therefore derived from the CBA for the Probability of Failure on Demand (PFD) of the AMAT device to be less than $1x10^{-3}$. The certification of the design of the device proving the reliability is a key part of the evidence and is used to support

the claim that “the FLCB device is designed to operate effectively and safely for all postulated network fault conditions and satisfies the derived Safety Requirements” (Claim C2).

The results of the trial will also further influence the design and development of maintenance schedules and operator instructions. These will be used to revalidate and update elements of the safety case prior to extended operations and ultimately BAU operation.

In summary this PSCR concludes that:

1. The hazards associated with the FLCB device are understood and sufficiently managed such that the operation and implementation of the device at the trials site can be considered to be ‘Safe’, whereby the risks have been reduced to a level that is either ‘Broadly Acceptable’ or ‘Tolerable and ALARP’.
2. Provided that the reliability of the FLCB device can be proven during the trial period, and that the risks associated with construction / installation are understood and will be adequately controlled, a suitable ‘case for safety’ can be made for operation of the FLCB device in BAU application such that the safety risks associated with the network equipment seeing a fault current above its rating can be ‘Broadly Acceptable’ or that the risk can be reduced to be ‘Tolerable’ and ‘ALARP’.

This PSCR has been produced to support both the trial and the BAU application. A number of evidence items, e.g. those to be generated during the trial, remain outstanding at the time of this issue. Where this is the case this has been highlighted in blue. Following the trial this PSCR will be updated and the CAE will be revisited to support BAU application.

ACRONYMS AND ABBREVIATIONS

ABB	ABB Group
ALARP	As Low As Reasonably Practicable
AMAT	Applied Materials Inc.
BAU	Business As Usual
CAE	Claims, Arguments and Evidence
CBA	Cost Benefit Analysis
DG	Distributed Generation
DNO	Distribution Network Operator
ECO	Engineering Change Order
ECR	Engineering Change Request
EPN	Eastern Power Networks
FCS	Fast Commuting Switch
FLCB	Fault Limiting Circuit Breakers
FMEA	Failure Mode and Effects Analysis
FWI	Fatality and Weighted Injury
HAZID	Hazard Identification
HAZOP	Hazard and Operability Study
HSE	Health and Safety Executive
IGBTs	Insulated Gate Bipolar Transistors
LPN	London Power Networks
NIC	Network Innovation Competition
NPI	New Product Introduction
PFD	Probability of Failure on Demand
PSCR	Preliminary Safety Case Report
QMS	Quality Management System
RA	Risk Assessment
RIDDOR	Reporting of Injuries, Diseases and Dangerous Occurrence
SCP	Safety Case Principles
SPN	South Eastern Power Networks
SQEP	Suitably Qualified and Experienced Personnel
UKPN	UK Power Networks

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 no more than first aid treatment either whilst at work or from a medical professional but does not result in a lost time injury.
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 8
1.1 BACKGROUND 8
1.2 SAFETY CASE REQUIREMENT 8
1.3 DOCUMENT PURPOSE 9

2. SCOPE OF THE SAFETY CASE 10

3. SYSTEM DESCRIPTION / USE CASES 11
3.1 TECHNICAL CHALLENGE 11
3.2 AMAT 250A FLCB 11
3.3 TRIAL 11

4. SAFETY CASE PROCESS AND PRINCIPLES 13
4.1 SAFETY MANAGEMENT PROCESS 13
4.2 SAFETY CASE PRINCIPLES 13
4.3 ACCEPTANCE CRITERIA 14

5. SAFETY CLAIMS, ARGUMENTS AND EVIDENCE 15
5.1 OVERVIEW 15
5.2 CLAIM C1 – SAFETY REQUIREMENTS 16
5.3 CLAIM C2 – FLCB DESIGN 20
5.4 CLAIM C3 – IMPLEMENTATION 25
5.5 CLAIM C4 - OPERATION 26
5.6 EVIDENCE SUMMARY 27

6. CONCLUSIONS 29

7. REFERENCES 30

ANNEX A - CLAIMS, ARGUMENTS, EVIDENCE DIAGRAMS 31

ANNEX B - SAFETY CASE EVIDENCE TABLE 37

ANNEX C - FLCB DEVICE SPECIFICATION 39

1. INTRODUCTION

1.1 BACKGROUND

Fault current limiting technologies can be used to solve the fault level constraints, presented by interconnection, short cable distances and other factors, which are limiting the growth of low-carbon generation on electricity distribution networks in Great Britain. Fault Limiting Circuit Breakers (FLCBs) provide a means to allow the continued growth and connection of distributed generation onto the distribution network in a cost-effective manner.

In developing the safety argument for the Applied Materials Inc (AMAT) 250A FLCB it is important to recognise that operation of the existing 11kV distribution network is not free from risk as there is the potential for arcing / flashovers or electric shock etc. from existing switchgear. These risks are well known and already managed and the introduction of the FLCB device is not expected to adversely affect them. However, the FLCB device does introduce a new safety risk in that with increased Distributed Generation (DG) there is the potential for network equipment to experience a fault current above its rating should the FLCB fail to operate on demand. The safety case presented herein considers this 'additional' risk and ultimately argues whether the risk can be reduced to be 'Tolerable and ALARP'.

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

- The first device, produced by ABB, is designed for deployment in primary substations.
- The second, produced by AMAT, is designed for direct connection to customer generators.

Parallel trials are being undertaken to provide an insight to stakeholders on the relative suitability of the two technologies, each in a suitable location, as well as provide 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.

The first device, produced by ABB, will be trialled at a primary substation and the second, produced by AMAT, at a customer generator site. The trials will not exceed the fault level limit however this scenario is a possibility in BAU. The risks associated with running the substation with fault levels above what the equipment is rated for are higher. Therefore the devices will need to be verified that they can reliably operate as described by the manufacturer before the devices can be extended from the trial to general use. For more details around the Annex C of this report.

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 also demonstrates that the safety management system (i.e. policy, organisation, documentation, training, performance monitoring, change control etc.) are 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, the Safety Case is 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 the Safety Case is based upon a feasibility study carried out by Frazer-Nash Consultancy (Frazer-Nash) in 2016 [7] for the ABB FLCB device. The assessment was underway before AMAT joined the project, and therefore only examined the ABB FLCB. Frazer-Nash understands that the two devices are similar; although they are intended to operate in slightly different locations in the 11kV network.

1.3 DOCUMENT PURPOSE

The purpose of this document is to present the safety argument for the AMAT 250A FLCB device to support the trials and to provide confidence that a ‘case for safety’ can be made for the BAU application.

2. SCOPE OF THE SAFETY CASE

Operation of the existing 11 kV distribution network is not free from risk as there is the potential for arcing / flashovers or electric shock etc. from existing switchgear. These risks are well known and managed and are considered to be 'Broadly Acceptable'. Introduction of the AMAT FLCB device is not expected to adversely affect this. However, the application for which the FLCB device is used is new and unique to the electricity network which introduces a new risk, as it allows the potential fault currents to exceed the ratings of some network equipment. The scope of the Safety Case is bound by the FLCB device itself, its functionality and the environment it will operate in. Initially, this will be constrained to a trial at one specific site but it also considers BAU operation on the wider 11kV network (i.e. a generic application case) in order to ensure that the Safety Case is comprehensive. This has been developed as part of the Safety Management process (see Section 4).

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 FLCB 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 demonstrates that the devices and their use in both trials and general application is 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 the relevant prescriptive Safety Requirements have been met. Adherence to the safety case principles (see Section 4.2) is used to determine whether a suitable 'case for safety' has been made.

3. SYSTEM DESCRIPTION / USE CASES

3.1 TECHNICAL CHALLENGE

A conventional circuit breaker interrupts fault current by physically separating its contacts, allowing the resulting voltage surge to form an arc between the contacts, then using various methods to extinguish the arc. A typical vacuum circuit breaker takes 40-60ms to open its contacts, then another 10-15ms to extinguish the arc, for a total interruption time of 50-75ms.

Conversely, a power electronic FLCB interrupts fault current by turning off Insulated Gate Bipolar Transistors (IGBTs), and uses a surge arrestor and snubber circuit to absorb the voltage surge without forming an arc. There are no moving parts or arc to interrupt, so the fault current can be interrupted within 2ms or less.

Existing FLCB technologies suffer from limitations caused by conduction losses, as the IGBTs that interrupt fault current also have to carry normal load current. This means that the current FLCBs need many IGBT modules to handle the current at full load; and/or need a large cooling system to dissipate heat at full load. Space requirements for existing FLCBs prevent their usage at London Power Networks (LPN) substations where space is usually limited and therefore block their consideration as a viable alternative to the proposed scheme.

The trial will be carried out on the LPN. However as previously mentioned and following a successful outcome, BAU installation may include installation onto the Eastern Power Network (EPN) and the South Eastern Power Networks (SPN).

3.2 AMAT 250A FLCB

AMAT is a world leader in supplying tools to the semiconductor fabrication industry. The ‘Fault Current Limiter Project’ has been running for eight years and has seen two technologies developed. One is based on superconductors and has seen four installations around the world, including two at 115kV recently energised in Thailand. The second is based on a solid state switches and mutual reactor. An installation demonstrating the switches alone (with low currents) has been installed in a novel ‘Bush Fire Prevention’ installation in Australia. AMAT are committed to identifying more mainstream demonstration applications.

AMAT’s 250A FLCB solution currently forms part of design for a 2000A solid-state fault current limiter, which uses a 250A interrupter combined with a current-limiting mutual reactor to minimise physical size and conduction losses. The project will trial the 250A FLCB by itself (without the reactor), installed in front of a customer’s generator at their premises to eliminate the generator’s contribution to the network fault level.

The FLCB at the customer premises will operate faster than the conventional circuit breakers on the substation, thereby eliminating the customers contribution to the effective fault levels that the substation circuit breakers would be required to break in case of a fault.

A detailed description of the AMAT 250A FLCB device is provided in Annex C.

3.3 TRIAL

To understand the main risks with the FLCB concept and try to mitigate them, as far as possible, during the design and verification phase several activities were initiated.

The completed FLCB device shall be tested in accordance with a comprehensive test and documentation plan mutually agreed by UKPN and AMAT. This covers the following:

- Power Frequency Voltage Withstand Test;

- Lightning Impulse Voltage, Switching Impulse Voltage and/or Chopped-Wave Lightning Impulse Voltage / Surge Current Test (Alternate);
- Partial Discharge;
- Control Circuit Design voltage and wiring checks;
- Rated Continuous Current (Type test);
- Short-Time Withstand Current and Peak Withstand Current Tests (Type test);
- Harmonic Distortion (Type Test);
- Short-circuit current limitation tests (Type Test);
- Current Interruption (Type test);
- Recovery (Type test);
- Electromagnetic Compatibility EMC (Type Test);
- Audible Sound (Type Test);
- Measurement of AC Magnetic fields (Type Test);
- Seismic tests (Type Test);
- Visual Inspection; and
- FCL Technology-Specific Tests.

Section 5.3.3 provides reference to the evidence of the verification activities and standardised testing that support the argument that the FLCB device has been tested and commissioned for use at the specified trial site.

4. SAFETY CASE PROCESS AND PRINCIPLES

4.1 SAFETY MANAGEMENT PROCESS

A Safety Case Process and Principles document [5] has been produced 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. An overview of the safety management process is shown in Figure 1. Details of how each step in the process has been used to develop the safety argument can be found in Section 5 of this Preliminary Safety Case Report (PSCR).

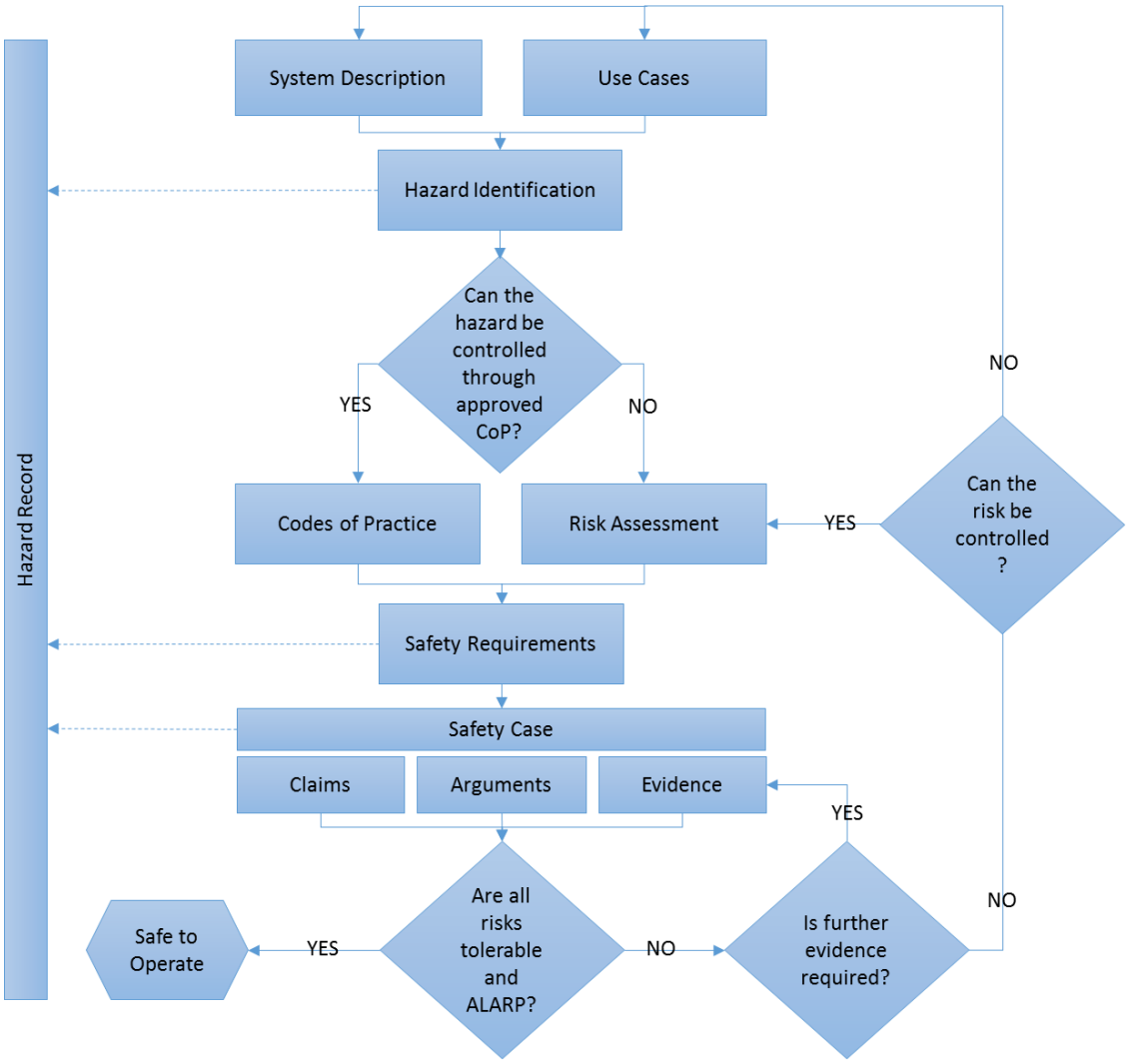


Figure 1: Safety Management Process

4.2 SAFETY CASE PRINCIPLES

The following high level safety case principles (SCPs) have been derived which have informed the case development process.

SCP 1 The Safety Case should demonstrate that the management system (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 of 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.

4.3 ACCEPTANCE CRITERIA

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. The Safety Case presents the safety argument to support the following 'Top Goal':

"The FLCB device and any required safety control shall be sufficiently reliable, or have suitable mitigation installed, such that the safety risks associated with the network equipment seeing a fault current above its rating is 'Broadly Acceptable' or that the risk has been reduced to be 'Tolerable and ALARP'.

5. SAFETY CLAIMS, ARGUMENTS AND EVIDENCE

5.1 OVERVIEW

The overall safety argument for the FLCB device is expressed using a "Claims, Argument and Evidence" (CAE) structure. 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, will result in the FLCB device having an acceptable level of safety. 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. The status of each piece of evidence is defined as:

- Green – A complete issued version of the evidence is held;
- Yellow – A draft version or a reference to the evidence is held; and
- Orange – No evidence currently exists.

The CAE approach allows the safety argument to be presented pictorially which shows the links between each piece of *evidence*, *argumen*t and *claim* that it supports. Figure 2 below provides a definition for each aspect and detail on how the diagram is presented.

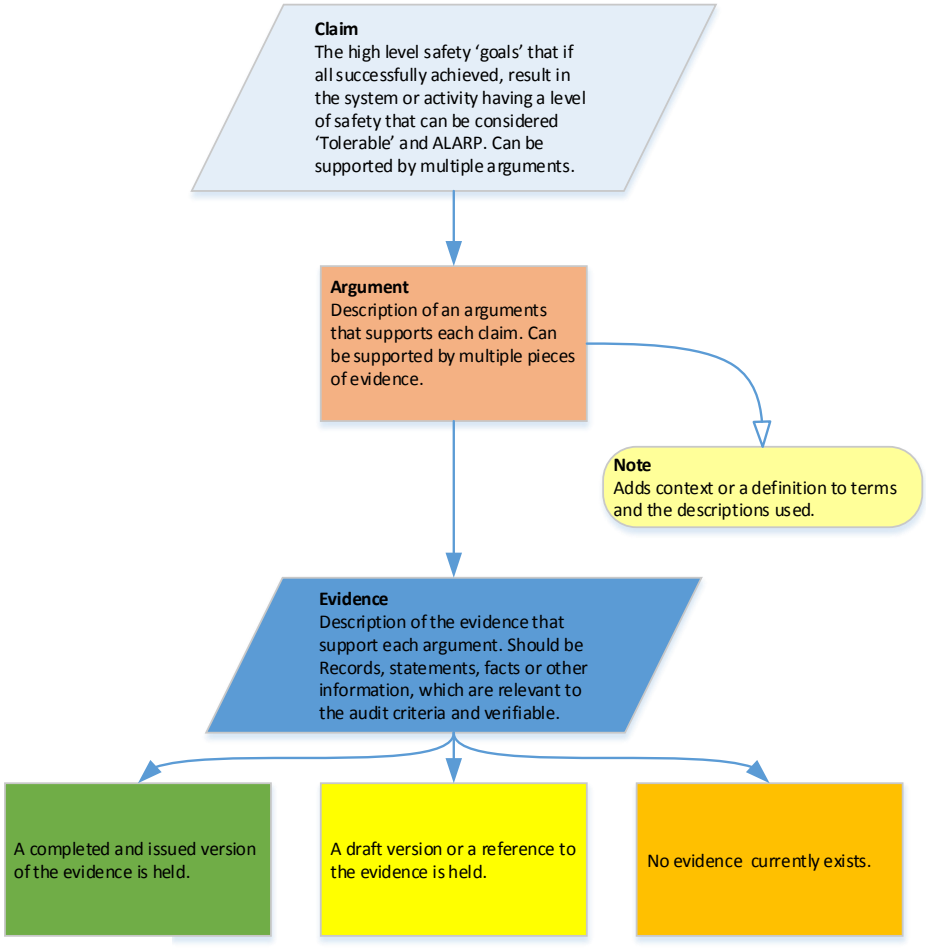


Figure 2: CAE Definition Diagram

The CAE diagram for the FLCB device can be found in Annex A.1 which identifies four key safety *claims (C1, C2, C3 and C4)* all supporting the overall "Top Goal".

The following sections present each safety claim, associated arguments and the evidence that supports it. Each piece of evidence can be found in the Safety Case Evidence Table in Annex B along with the associated reference and evidence status.

5.2 CLAIM C1 – SAFETY REQUIREMENTS

"A suitable and sufficient safety assessment process has been undertaken and appropriate Safety Requirements have been derived."

The Safety Management process is defined in the Safety Case Process and Principles document [5] and is summarised in Section 4.1 of this Report. This Section details how each individual step is used to produce the safety case for the FLCB device.

5.2.1 Argument (C1A1)

"The FLCB device and its use case has explicitly been defined and described."

In order to bound the scope of the Safety Case it is important to explicitly define and describe the AMAT FLCB device and its use case. This ensures that the activities undertaken to develop the Safety Case are well focussed and provide credible evidence to the process.

A detailed description of the AMAT FLCB Device can be found in Annex C of this Report.

Evidence (C1A1E1)

"Technical specifications have been produced which set out the requirements for the device and systems related to the Powerful-CB project."

The Standard for Indoor 12kV Power-Electronic Fault-Limiting Circuit Breakers [E21] sets out the requirements for indoor power-electronic fault-limiting circuit breakers being trialled as part of the Powerful-CB project.

The Standard for Indoor 12kV, 24kV and 36kV Metal Enclosed Switchgear for Grid and Primary Substations [E22] sets out the requirements for indoor switchgear at these substations for UKPN.

Evidence (C1A1E2)

"*A description document of the device has been produced by AMAT"*

The AMAT FLCB Device Equipment Reference Manual [E17] includes a detailed description of the device and its use cases.

5.2.2 Argument (C1A2)

"A systematic approach has been used to identify all reasonably foreseeable hazards that apply to the 'system' together with potential initiating events or sequences of events."

The purpose of the Hazard Identification (HAZID) undertaken is to identify all reasonably foreseeable hazards which are then assessed. The HAZID should be systematic and structured. Correct HAZID underpins the whole risk management process and gives assurance that the risks will be managed in the project.

The HAZID Workshop was held on 20th June 2017 at the Frazer-Nash offices in Dorking. The workshop was conducted using a 'guide word examination' technique which is a deliberate search for deviations from the design intent. Attendees were asked to apply a series of

'Guidewords' in conjunction with 'Parameters' to each 'Node' to generate deviations from the design intent which can lead to undesirable consequences.

This HAZID workshop was chaired and staffed by Suitably Qualified and Experienced (SQEP) persons, and a record of their relevant qualifications and experience kept. Prior to commencement of the workshop, the team present was assessed by the HAZID Chairman to confirm they are SQEP.

Evidence (C1A2E1)

"A HAZID workshop was undertaken to identify hazards for the FLCB device in both trials and general application."

The full output of the workshop is contained within the HAZID Workshop Report [E2].

The HAZID workshop was preceded by a Briefing Note [E1] which described the system and scope to be considered and the methodology being proposed for use in that workshop.

The hazards and all accompanying information identified during the workshop have been used to create the project Hazard Record [E3].

Evidence (C1A2E2)

"The HAZID was carried out by SQEP individuals."

An attendance sheet is shown in the HAZID Workshop Report [E2] and signed SQEP forms for each attendee are held separately on record by Frazer-Nash.

5.2.3 Argument (C1A3)

"Methodology and evaluation criteria adopted for the risk assessment is clear and has been developed specifically for the use of AMAT FLCB devices on the electricity distribution network"

For assessment of risk for the use of the AMAT FLCB device on the electricity distribution network a risk classification matrix is used which defines the boundaries between the 'Unacceptable', 'Tolerable' and 'Broadly Acceptable' regions for both the exposed worker (staff or contractors) and the general public.

The risk matrix has been developed specifically for use of the FLCB device on the electricity distribution network. This is based on the Health and Safety Executive (HSE) upper limit of tolerability for individual risk per annum for workers and for members of the public and calibrated specifically to the risk associated with the FLCB, accounting for the specific hazards and exposure size in question.

Evidence (C1A3E1)

"The risk classification matrix and acceptance criteria are documented and communicated to relevant stakeholders"

The risk classification matrix, including details of its derivation, are detailed in the Safety Case Process and Principles Document [E5].

Consequences used in the risk classification matrices relate to personal injury, property damage and environmental impact are taken from UKPN Incident Reporting Procedure [E18].

5.2.4 Argument (C1A4)

"A suitably sufficient and robust process has been undertaken to evaluate and assess safety risks and identify reasonably practicable Safety Measures"

The Risk Assessment followed on from the HAZID activities as an essential part of the hazard management process in order to assess whether the risks arising from use of the two FLCB devices on the 11kV network can be controlled to levels which are Tolerable and ALARP.

Three main consequences were identified, these are:

- Network exposed to excessive fault current;
- Flashover / local explosion; and
- Electric shock.

The Risk Assessment (RA) workshop, held on the 27th September 2017, focused on assessing the consequences and any secondary consequences which may follow. Each consequence was assessed to determine the exposure group, severity in terms of harm, asset damage and environmental damage and the likelihood of occurrence.

The workshop then identified any other potential Safety Measures that could be implemented to reduce the risk to a level that is tolerable and ALARP.

The RA workshop was chaired and staffed by SQEP persons, and a record of their relevant qualifications and experience kept. Prior to commencement of the workshop, the team present was assessed by the Workshop Chairman to confirm they are SQEP.

It was determined that the likelihood of flashover following installation of the FLCB devices or an electric shock from the FLCB device is no different from any other type of switch gear. The same controls apply based on switchgear construction standards, relevant good practice of current switchgear and following current procedures. As such these safety risks can be considered to be 'Broadly Acceptable'.

However, it was recognised that a disruptive failure of a circuit breaker due to the network being exposed to excessive fault current would pose a risk that is different to what is currently present. This risk was therefore agreed to be investigated further using a CBA.

Evidence (C1A4E1)

"A Risk Assessment workshop was undertaken to assess risks of implementing the FLCB device on the network and to identify potential Safety Measures"

The full output of the workshop is contained within the RA Workshop Report Issue 1 [E6].

The RA workshop was preceded by a Briefing Note [E7] which described the system and scope to be considered and the methodology being proposed for use in that workshop.

The Safety Measures and all accompanying information identified during the workshop have been used to create the project Hazard Record [E3].

Evidence (C1A4E2)

"RA Workshop was carried out by SQEP individuals."

An attendance sheet is shown in the RA Workshop Report Issue 1 [E6] and signed SQEP forms for each attendee are held separately on record by Frazer-Nash.

5.2.5 Argument (C1A5)

"Cost Benefit Analysis has been carried out, using recognised methodologies and robust data, to determine whether potential Safety Measures are necessary to ensure safety so far as is reasonably practicable."

CBA can be used as part of ALARP decisions and aids the decision making process by giving monetary values to the costs and benefits, including safety benefits, of various options. This enables a comparison of the advantages and disadvantages of multiple options to be compared using the 'like quantity' of financial value.

The CBA is based on findings from the RA workshop held on the 27th September 2017. It evaluates the safety mitigations identified at the Workshop and uses data sourced from multiple Actions raised at the Workshop.

The CBA determines whether the cost to implement the additional Safety Measures identified in the RA workshop is grossly disproportionate to the safety benefit obtained. This informs the ALARP decision for the risk of a 'Disruptive Failure of Circuit Breaker'.

Two potential Safety Measures were identified in the RA workshop, these are:

- Option 1 – Fast Fuse; and
- Option 2 – Automated Self Tests.

However, in undertaking the CBA the viability of the options was challenged and, after initial testing, Option 1 (Fast Fuse) was found to be no longer feasible as the fuse requires too much energy to be certain of clearing before a first peak.

Option 2 (Automated Self Tests) does not result in any risk reduction but instead may help increase the likelihood of the device meeting the PFD Safety Requirement. This 'Safety Measure' was therefore not included in the CBA as it is only required in so far as it is needed to meet the PFD Safety Requirement already derived in the CBA.

Evidence (C1A5E1)

"The input data used in the CBA is accurate and relevant"

The data used for the CBA is listed in Appendix C of the RA workshop Report Issue 2 [E19] each supplemented with a reference.

Evidence (C1A5E2)

"The CBA was conducted in accordance with recommended good practice"

The RA workshop Report Issue 2 [E19] summarises the outputs of the RA Workshop and details the findings of the CBA. It contains an analysis and comparison against the existing network and baseline option. Sensitivity analysis was used to ensure suitably cautious assumptions have been made and allows the robustness of the outcomes of the CBA to be assessed.

The Safety Measures and all accompanying information identified during the workshop are detailed in the project Hazard Record [E3].

5.2.6 Argument (C1A6)

"Safety requirements have been derived from relevant applicable policies, procedures or regulations and the Risk Assessment."

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 and assessed. Where relevant, control measures identified by the hazard management process are designated as Safety Requirements. Safety requirements have also been derived from the relevant applicable policies, procedures or regulations.

Hazards may also be suitably controlled though the application of UKPN policies and procedures or by adherence to Regulations. Where this is identified as being the case no further risk assessment was undertaken. Where these risks were not covered, Safety Requirements were formed from the RA and CBA.

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 the device. Safety requirements and evidence of compliance against them is held within the Hazard Record.

Evidence (C1A6E1)

"*A HAZID workshop was undertaken which derived the Safety Requirements.*"

The full output of the workshop is contained within the HAZID Workshop Report [E2].

Evidence (C1A6E2)

"A Risk Assessment workshop and CBA was undertaken which derived Safety Requirements."

The full output of the workshop and subsequent CBA is contained within the RA Workshop Report Issue 2 [E19].

Evidence (C1A6E3)

"*A Hazard Record has been developed which details the Safety Requirements*."

A Hazard Record [E3] has been produced for the AMAT device to capture the output from HAZID and RA activities. The Hazard Record is a live document and is continually updated throughout the project.

5.2.7 Argument (C1A7)

"The outputs from all safety related activities are recorded and continually updated throughout the project"

The Hazard Record will remain live and continue to be managed throughout the project. It records the outputs from the HAZID activities, RA and Safety Measures / Safety Requirements. Following this it will be used to track the project progress against the following:

- Actions raised at the various safety related activities that may be used to form a Safety Requirement.
- Compliance with relevant policies, procedures or regulations.
- Safety requirements by referencing evidence demonstrating that they have been implemented.

Evidence (C1A7E1)

"*A Hazard Record has been developed and is continually updated throughout the project*."

A Hazard Record [E3] has been produced for the AMAT device to capture the output from HAZID and RA activities. The Hazard Record is a live document and is continually updated throughout the project.

5.3 CLAIM C2 – FLCB DESIGN

"*The FLCB device is designed to operate effectively and safely for all postulated network fault conditions and satisfies the derived Safety Requirements."*

The engineering processes are included as part of the Quality Management System (QMS). This project follows the New Product Introduction (NPI) engineering process. The full scope of the QMS engineering design processes are as follows:

- The NPI Engineering (QMS Process 03.3-02-134) process uses the Engineering Design Process for the development of new products.
- The Engineering Change Order (ECO) Process (QMS Process 03.3-02-23) defines the process to create, develop, and submit the Engineering Change Request (ECR)/ ECO.
- The DFx Process (old QS-14) defines a formalised integration of internal customers into High Level and Detail Design.
- The EARS Database Process (QMS Process 03.4-01-28) defines the generation of CIP projects.
- The Failure Analysis and Corrective Action Process (QMS Process 05.4-02-09) defines the use of the QN system.

The NPI process contains five major phases:

1. Project Definition and Requirements;
2. High Level Design;
3. Detailed Design;
4. Test and Verification; and
5. Design Implementation.

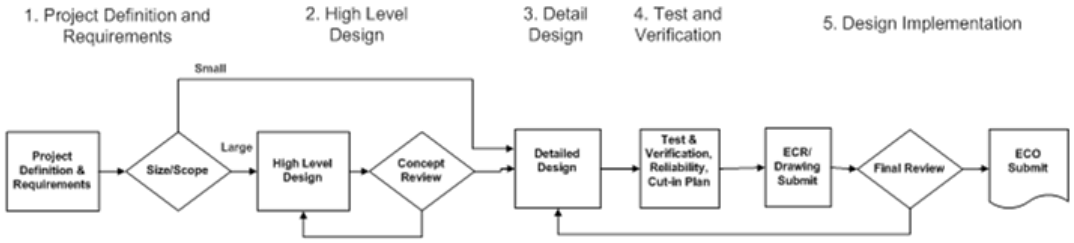


Figure 3: New Product Introduction Process

A key feature of the design process is the review stage, the two types deployed are:

- Cross Functional Reviews; held at the High Level Design and at the Design Implementation phases. These reviews focus on informing Safety, Production Control, Product Support, Manufacturing, Production Implementation and Final Test of the changes.
- Functional Design Reviews; held after the Detailed Design phase and before parts are procured. These reviews focus on the technical aspects of the change and include a detailed review of part drawings with respect to Best Known Methods.

Supporting information around the design of the FLCB device can be found in Annex A of this report. This Section details the activities associated with the development process of the design of the FLCB device so to meet the Safety Requirements.

5.3.1 Argument (C2A1)

"The FLCB device has been designed by competent designers to operate effectively and correctly."

The FLCB device has been designed to operate satisfactorily for the system parameters and meets the various design requirements set out in the applicable standards.

Due to the nature of the device and the environment that it will be used in safety has been considered through all stages of the project. Principles such as 'Diversity' and 'Redundancy' have been considered when designing the device and the system so to enhance the integrity and reliability of safety systems.

As mentioned above, numerous QMS processes are followed to ensure the device is designed to support this argument.

Evidence (C2A1E1)

"*Internal UKPN Standards have been followed to ensure the device and associated equipment to be installed at the Grid and Primary substations operate effectively and correctly."*

The standard for Indoor 12kV Power-Electronic Fault-Limiting Circuit Breakers [E21] lists a number requirements for the design and construction of the FLCB device. The standard for Indoor 12kV, 24kV and 36kV Metal Enclosed Switchgear for Grid and Primary Substations [E22] lists additional design requirements and requirements for the maintenance and operation of the device. This equipment shall be designed to meet the normal service conditions for indoor switchgear and controlgear as specified in clause 2.2 of ENA TS 41-36.

Evidence (C2A1E2)

"AMAT FLCB Design Report"

The Design Report [E8] is still TBC.

5.3.2 Argument (C2A2)

"The designers have been integral to the safety assessment process and able to influence the design during the development."

The project has undertaken a series of safety assessment activities using a wide range of design expertise throughout. This has ensured the design of the device controls the risks associated and complies with relevant statutory provisions.

It is important to note that an integrated, safety-led approach has been adopted to the development of the design, and that the design development can be iterative. Reasons that a number of iterations may be required include, but are not limited to:

- Changes to the functional requirements or Safety Requirements;
- The discovery challenges to the design in the HAZID;
- The results of testing and validation; and
- The results of trials and substantiation.

Evidence (C2A2E1)

"Designers have attended the HAZID and RA Workshops and had opportunities to review of the outputs"

The full output of the workshop is contained within the HAZID Workshop Report [E2].

The RA workshop Report Issue 2 [E19] summarises the outputs of the RA Workshop and details the findings of the CBA. It contains an analysis of the two identified potential Safety Measures and comparison against the existing network and baseline option.

Each workshop has had the SQEP personnel available to produce the required outputs. AMAT have attended both the HAZID Workshop held on the 21st June 2017 and the RA Workshop held on the 27th September 2017. AMAT have had consistent communication with the project and have been responsible for numerous actions raised at the workshops.

5.3.3 Argument (C2A3)

"The FLCB device has been tested and commissioned for use at the specified trial site"

Before proceeding with trials, the following activities ensure that it is safe to do so. Activities at this stage include:

- Confirm that the FLCB has been successfully built in accordance with the detailed design;
- Specify the testing required to confirm the functionality and safe operation of the FLCB;
- Establish any limitations of use for the trial period;
- Identify situations that involve personnel working on sites or in conditions that they are not familiar with;
- Review the HAZOP, Failure Mode and Effects Analysis (FMEA) and fault tree analysis as applicable to check this is all still relevant and correct.

At this point, substantiation of the Safety Requirements related to the device performance have not been achieved: evidence from the trial period will be key in doing so. However, there is sufficient evidence from the previous testing and validation stages to ensure that the FLCB device can be safely implemented on the network, and that the risks associated with installation and commissioning are ALARP. This forms the basis of the installation and commissioning safety arguments in the in-service safety case.

This stage may recommend further testing or analysis before the device is considered safe to put on the network. Although less likely as the process develops, it may also identify further design changes.

Evidence (C2A3E1)

"Testing and commissioning of the FLCB device has been completed to ensure it meets its functional and safety requirements"

Key components of the design are tested by the tests listed in Section 3.3.

Evidence for the Testing and Commissioning of the AMAT FLCB device can be found in document [E9].

Evidence (C2A3E2)

"Reliability data and FMEA support the testing and commissioning of the device and trial site for safe implementation."

The Reliability data and FMEA can be found in document [E20].

5.3.4 Argument (C2A4)

"The FLCB device meets the legislative Safety Requirements"

Relevant legislation has derived a number of Safety Requirements for the FLCB device. Some hazards are suitably controlled through the application of UKPN policies and procedures (e.g. application of distribution safety rules) or adherence to Regulations (e.g. compliance with Electricity at Work Regulations). Where it has been identified that the device meets these requirements no further risk assessment was undertaken and compliance is recorded in the Hazard Record.

To prove compliance to the relevant standards, key components of the design are tested, See Section 3.3.

Evidence (C2A4E1)

"Legislative compliance statements have been authored"

A Hazard Record [E3] has been produced for the AMAT FLCB device which includes the relevant policies and procedures regulations. The Hazard Record is a live document and is continually updated throughout the project.

5.3.5 Argument (C2A5)

"The design of the FLCB device satisfies the derived Safety Requirements"

In order to demonstrate that the 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 have been identified. Where relevant, control measures identified by the hazard management process have been designated as Safety Requirements. Compliance against these requirements is a key part of the evidence needed to build the safety case and therefore form part of the basis of the acceptance criteria for the laboratory and field trials for the device.

Safety requirements for the FLCB device ensure it performs in a safe manner when installed on the trial network or as BAU. Safety activities such as the FMEA and reliability assessments prove compliance against the derived Safety Requirements.

Evidence (C2A5E1)

"The FLCB device meets the derived Safety Requirements"

One of the key parameters in the safety and reliability considerations is the Probability of Failure on Demand, meaning the probability of the device failing to perform its safety function at a given command. The required PFD that needs to be achieved or exceeded is a Safety Requirement derived from the risk assessment. The estimation of the achieved PFD for the device is done by considering existing performance data (where available) together with test results from verification testing during the design and verification phase.

The reliability data and FMEA document [E20] prove that the device's performance and the system it is to be installed upon meet the derived Safety Requirements and is safe for installation on the trial and as BAU.

A Hazard Record [E3] has been produced for the AMAT device which lists each Safety Requirements against its relevant risk. It is provides a reference to the evidence for compliance against each Safety Requirements.

5.3.6 Argument (C2A6)

"The Data gathered during the trials will further substantiate the Safety Case"

Not all data is known about the performance of the AMAT FLCB device and hence before the device is installed to be used as BAU a trial is being carried out. This trial will provide sets of performance data which will be used to determine whether the device will operate reliably and safely as required for BAU.

Evidence (C2A6E1)

"Trial Reports for the AMAT FLCB Device"

The Trials are still to be undertaken and a report [E10] will be produced once completed.

5.4 CLAIM C3 – IMPLEMENTATION

"The AMAT FLCB devices can be implemented safely onto the electricity networks"

Sufficient evidence is needed from the safety assessment process to ensure that the FLCB device can be safely implemented onto the network in line with the Commission Implementing Regulations [6]. This Section presents the various arguments and evidence that ensure the device is considered safe to put on the network in the trials.

5.4.1 *Argument (C3A1)*

"*A safe installation strategy has been developed for the trial"*

The purpose of the installation strategy is to offer a safe, efficient and structured approach to installing the FLCB devices onto the electricity network.

It is important to note that an integrated, safety-led approach has been adopted to the development of the system design, and that the design development can be iterative. Reasons that a number of iterations may be required include, but are not limited to:

- Changes to the functional requirements or Safety Requirements;
- The discovery challenges to the design in the hazard identification;
- The results of testing and validation; and
- The results of trials and substantiation.

Evidence (C3A1E1)

"Installation Strategy Report has been produced for the FLCB device."

The full installation strategy is contained within the Installation Strategy Report [E11].

5.4.2 *Argument (C3A2)*

"The commissioning activities verify that the FLCB devices have been installed in accordance with the strategy."

Following installation of the devices onto the network the commissioning activities will verify that the as installed device is in accordance with the strategy and therefore meets the requirements for safe operation.

Evidence (C3A2E1)

"Installation and Commissioning Report has been produced."

The full Network Installation and Commissioning procedure and outputs are contained within the Installation and Commissioning Report [E12].

5.4.3 *Argument (C3A3)*

"Specific precautions are in place for the trial of the FLCB device on the electricity network."

Due to the nature of the device, specific precautions are in place to allow for safe operation. As such the potential fault current limit of the network at present will not be exceeded. However, it is important that the full FLCB capability needs to be extensively tested in a representative scenario to gain confidence in its operation for its use in BAU application i.e. with increased fault current levels.

Evidence (C3A3E1)

"A Trial Installation Strategy Report has been produced."

The full installation strategy is contained within the Installation Strategy Report [E11].

5.4.4 *Argument (C3A4)*

"There is sufficient resources to support the implementation of the FLCB Device for the trial and BAU."

The trial will require extra workforce and an analysis team, however it should not be done in a way that creates an un-realistic environment that is unsustainable during BAU.

Evidence (C3A4E1)

"Resource plan for the implementation of the FLCB device for both the Trial and BAU has been produced."

A plan [E13] identifying the required workforce and resources for the trial of the AMAT device has been produced.

5.5 CLAIM C4 - OPERATION

"The safe operation of the FLCBs can be sustained throughout the trial, the workforce is capable of delivering and assuring what is expected and they are supported by accurate asset information."

It is necessary that the risks of the FLCB device in normal operation do not introduce any unexpected or additional safety risks. This Section presents the arguments and evidence to support the safe operation of the FLCB device on the network.

5.5.1 *Argument (C4A1)*

"The workforce is trained and competent to discharge their duties."

Implementation of the devices onto the network for both the trial and BAU will require trained and competent personnel. This is to ensure a safe installation and that the devices operate as intended which will reduce risks in future operations.

Evidence (C4A1E1)

"Training schedule and documents have been produced and competence management framework is in place to deliver a capable workforce."

Details of the training, specific training documents and the competence framework can be found in the Training and Competence Plan [E14].

5.5.2 *Argument (C4A2)*

"Sufficient and appropriate resources are available to enable the workforce to discharge their duties."

For safe and efficient operation trained and competent personnel must be available for the required tasks for BAU.

Evidence (C4A2E1)

"A Resource plan has been produced to ensure resource needs requirements and appropriate tools are in place and available when required."

A Resource Plan [E13] identifying the required workforce and resources for the trial of the AMAT device has been produced.

5.5.3 Argument (C4A3)

"A fit for purpose assurance management system exists."

For safe installation, maintenance and operation an assurance management system must be in place.

Evidence (C4A3E1)

"Contractors operate robust assurance regimes that monitor and assess the performance of the FLCB devices."

The Assurance Management System document [E15] contains the details of the robust assurance regimes that contractors adhere to.

5.5.4 Argument (C4A4)

"The state of the infrastructure at any point in time is defined and available."

For safe installation, maintenance and operation the state of the infrastructure must be known.

Evidence (C4A4E1)

"Infrastructure Reports are produced and include any planned changes"

Details of the status and any planned changes to infrastructure are contained within the Infrastructure Reports [E16].

5.6 EVIDENCE SUMMARY

Annex B of this report lists each piece of evidence which is used to support the augments and claims made in Section 5.

Claim 1 contains arguments supporting the safety assessment of the device. Various safety activities undertaken as part of the project and supporting documents support this claim. The documents provide clear and concise arguments as listed in Section 5.2. This claim is still missing a Device Description for the AMAT FLCB Device to help substantiate the argument that the device and its use case has been explicitly defined and described. This will be produced prior to the commencement of the trials.

Claim 2 is supported by arguments which prove the device meets the Safety Requirements. The reliability of the device is based on predicted data, which is less robust than trials data, and hence the need for the trials before implementing the devices on the network for BAU. The trials will then substantiate the Safety Requirements derived from the predicted data. Evidence currently missing to support this claim include an AMAT FLCB Design Report, Reliability Data and FMEA Document and a Trial Report for the Device. The first three will be produced prior to the commencement of the trials and the fourth following the completion of the trials.

Claim 3 is supported by arguments detailing how the devices will be installed onto the network. Large evidence gaps still exist involving plans, schedules and strategies detailing how this will

be completed. It considers this for both the trial and for BAU and includes an Installations Strategy, Installation and Commissioning Report and a Resource Plan for the trial. These evidence documents will be produced prior to installation works for the trial.

Claim 4 relates to the safe operation and maintenance of the devices. Evidence still to be provided to support this claim include a Training and Competence Plan, an Assurance Management System Document and an Infrastructure Report. These evidence documents will be produced after the completion of the trials.

6. CONCLUSIONS

The safety activities undertaken as part of this process have supported a safety-led approach to the development of the system design and the safety case.

Following HAZID and RA Workshops, the likelihood of either a Flashover / Local Explosion or Electric Shock as a result of a fault with the FLCB device was agreed to be no different to any other type of switchgear that is currently installed on the network. Therefore the risk is no different and should be considered 'Broadly Acceptable' on this basis.

However, outside the trial, the consequence of the network being exposed to excessive fault current could lead to the disruptive failure of a circuit breaker and potentially result in an explosion within the sub-station and lead to a fire with an oil circuit breaker present. A risk assessment was undertaken to assess the tolerability of this risk and a CBA was undertaken on various potential Safety Measures to support a decision as to whether these risks are ALARP. The analysis concluded that, due to the high reliability of the devices, the safety risk is tolerably low and the cost to implement either of the two potential Safety Measure options is grossly disproportionate to the safety benefit gained.

The high reliability of the device is therefore crucial to the validity of this analysis and thus the safety case. A key Safety Requirement was therefore derived from the CBA for the PFD of the AMAT device to be less than $1x10^{-3}$. The certification of the design of the device proving the reliability is a key part of the evidence and is used to support the claim that "the FLCB device is designed to operate effectively and safely for all postulated network fault conditions and satisfies the derived Safety Requirements" (Claim C2).

During the trials the potential fault current limit of the network will not be exceeded, therefore the potential safety measures identified at the RA workshop to mitigate this are not required. In addition, the FLCB will have adjacent conventional circuit breakers. Therefore the risk can be considered to be no worse than existing operations and the protection is beyond that used in the usual design scope. However, it is important that the full FLCB capability needs to be extensively tested in a representative scenario to gain confidence in its operation for its use in BAU application i.e. with increased fault current levels.

The results of the trial will also further influence the design and development of maintenance schedules and operator instructions. These will be used to revalidate and update elements of the safety case prior to extended operations and ultimately commercial operation.

In summary this PSCR concludes that:

1. The hazards associated with the FLCB device are understood and sufficiently managed such that the operation and implementation of the device at the trials site can be considered to be 'Safe', whereby the risks have been reduced to a level that is either 'Broadly Acceptable' or 'Tolerable and ALARP'.
2. Provided that the reliability of the FLCB device can be proven during the trial period, and that the risks associated with construction / installation are understood and will be adequately controlled, a suitable 'case for safety' can be made for operation of the FLCB device in BAU application such that the safety risks associated with the network equipment seeing a fault current above its rating can be 'Broadly Acceptable' or that the risk can be reduced to be 'Tolerable' and 'ALARP'.

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

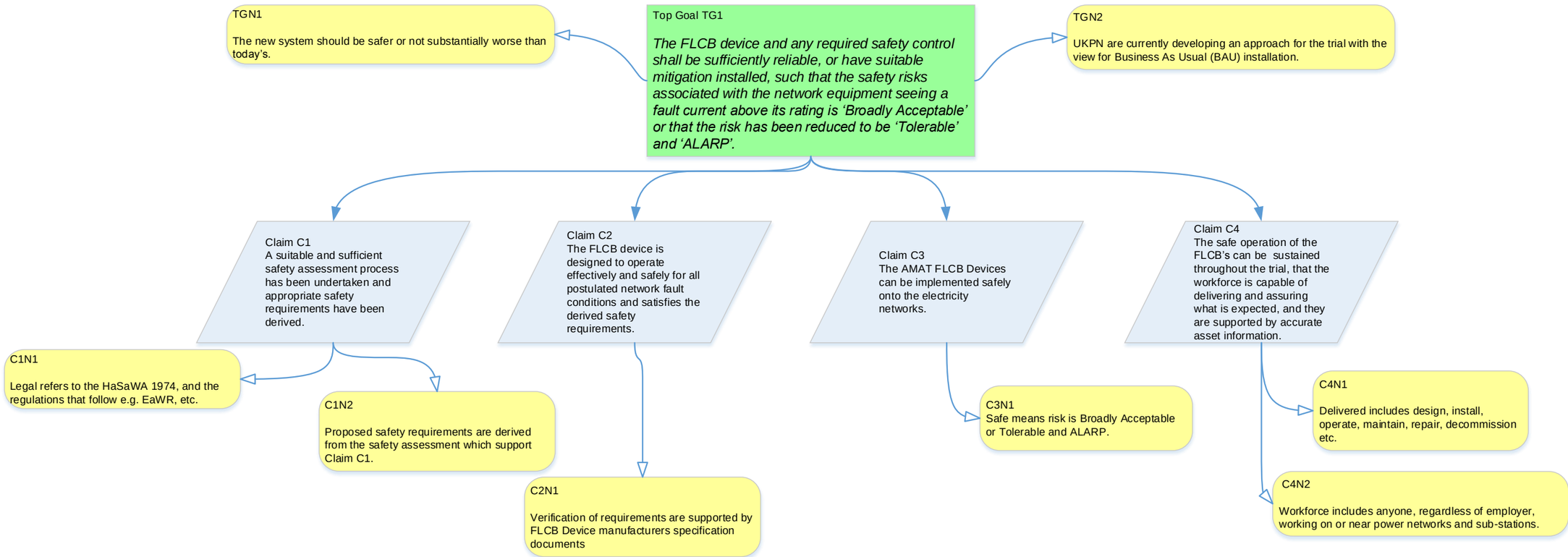
[4] The Electricity Safety, Quality and Continuity Regulations 2002

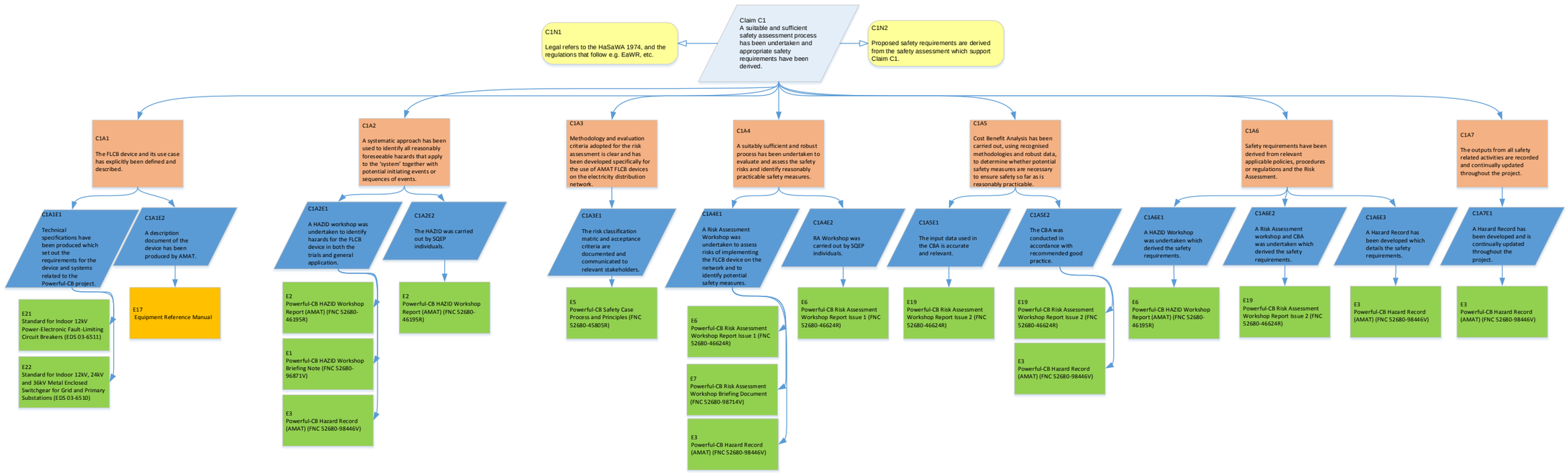
[5] FNC 52680-45804R, Powerful-CB Safety Case Process and Principles, Issue 1, 5th May 2017.

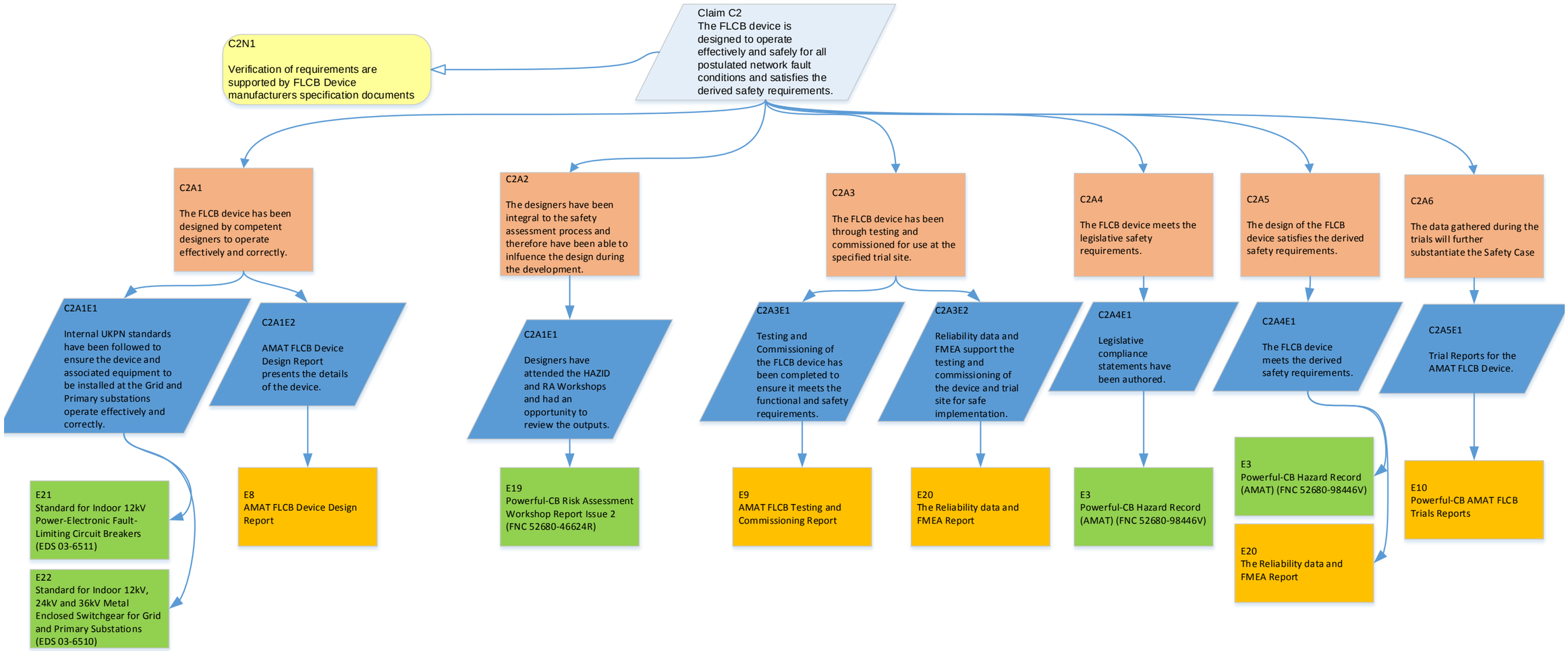
[6] Commission Implementing Regulations (EU) 2015/1136 amending Implementing Regulation (EU) No. 402/2013 on the Common Safety Method for Risk Evaluation and Assessment.

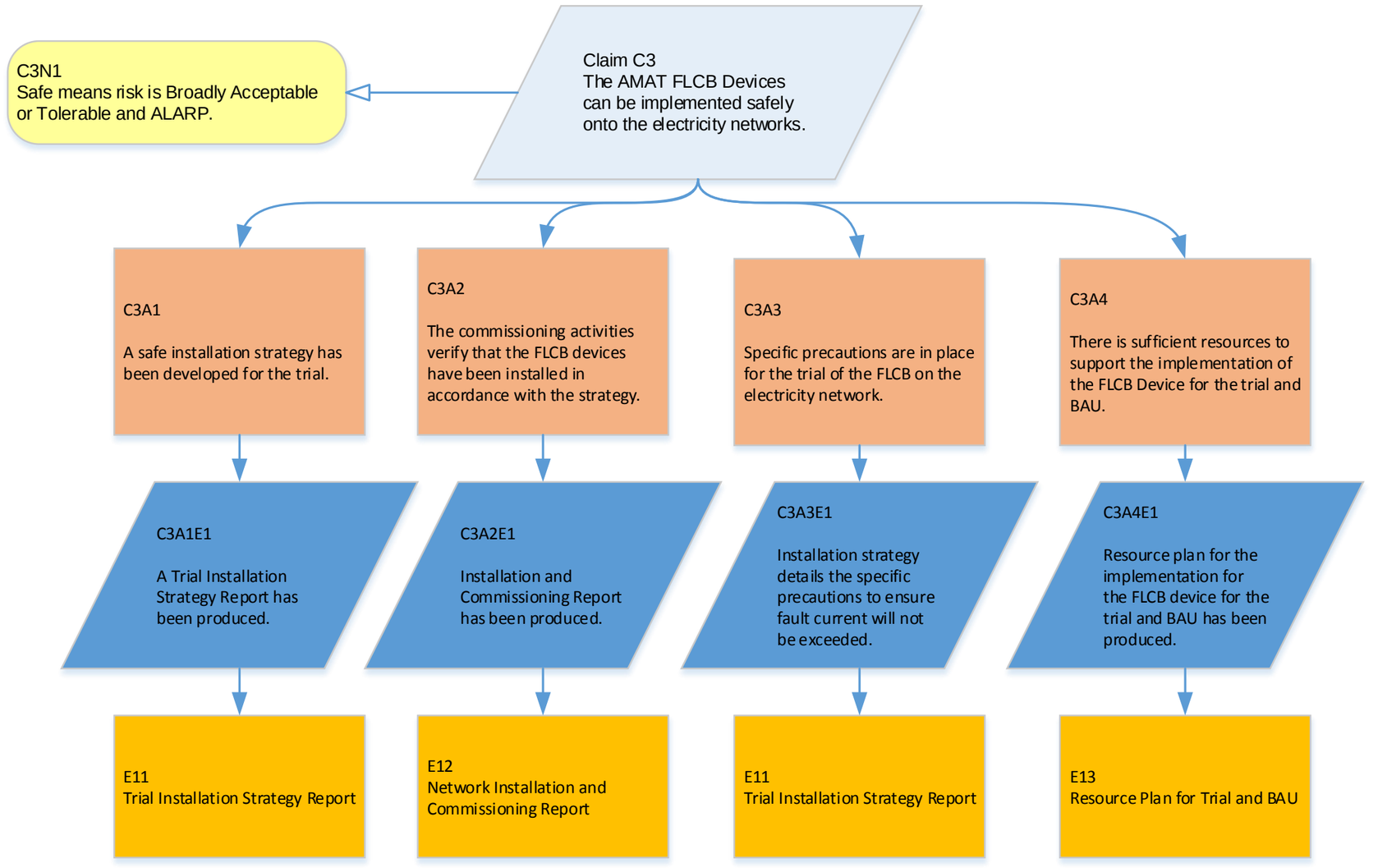
[7] FNC 50235/44699R Feasibility of safety case for ABB hybrid fault current limiter, 2016.

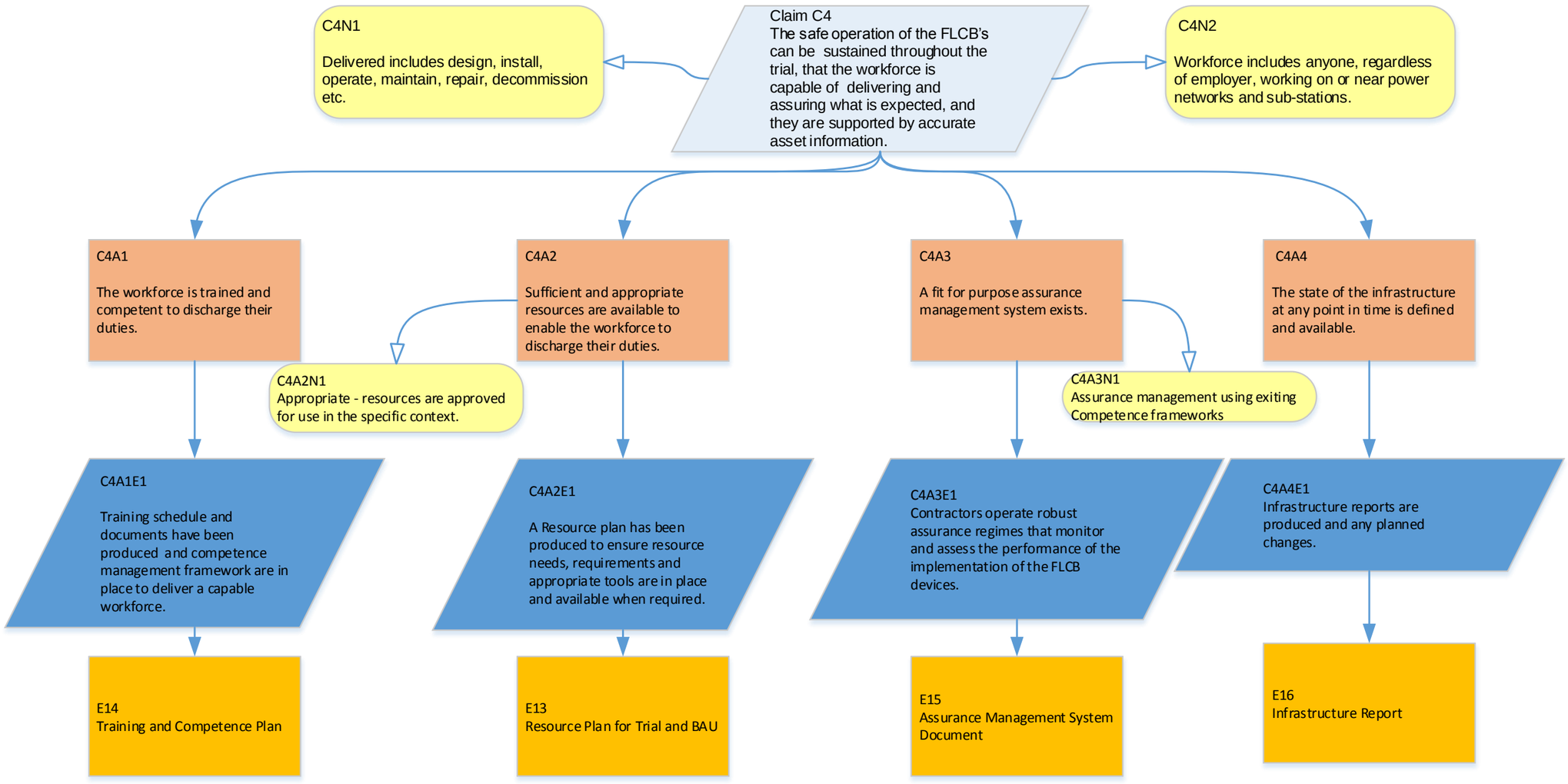
ANNEX A - CLAIMS, ARGUMENTS, EVIDENCE DIAGRAMS


TGN1
The new system should be safer or not substantially worse than today's.
Top Goal TG1
The FLCB device and any required safety control shall be sufficiently reliable, or have suitable mitigation installed, such that the safety risks associated with the network equipment seeing a fault current above its rating is 'Broadly Acceptable' or that the risk has been reduced to be 'Tolerable' and 'ALARP'.
TGN2
UKPN are currently developing an approach for the trial with the view for Business As Usual (BAU) installation.
Claim C1
A suitable and sufficient safety assessment process has been undertaken and appropriate safety requirements have been derived.
Claim C2
The FLCB device is designed to operate effectively and safely for all postulated network fault conditions and satisfies the derived safety requirements.
Claim C3
The AMAT FLCB Devices can be implemented safely onto the electricity networks.
Claim C4
The safe operation of the FLCB's can be sustained throughout the trial, that the workforce is capable of delivering and assuring what is expected, and they are supported by accurate asset information.
C1N1
Legal refers to the HaSaWA 1974, and the regulations that follow e.g. EaWR, etc.
C1N2
Proposed safety requirements are derived from the safety assessment which support Claim C1.
C2N1
Verification of requirements are supported by FLCB Device manufacturers specification documents
C3N1
Safe means risk is Broadly Acceptable or Tolerable and ALARP.
C4N1
Delivered includes design, install, operate, maintain, repair, decommission etc.
C4N2
Workforce includes anyone, regardless of employer, working on or near power networks and sub-stations.


Claim C1
A suitable and sufficient safety assessment process has been undertaken and appropriate safety requirements have been derived.
C1N1
Legal refers to the HaSaWA 1974, and the regulations that follow e.g. EaWR, etc.
C1N2
Proposed safety requirements are derived from the safety assessment which support Claim C1.
C1A1
The FLCB device and its use case has explicitly been defined and described.
C1A1E1
Technical specfications have been produced which set out the requirements for the device and systems related to the Powerful-CB project.
C1A1E2
A description document of the device has been produced by AMAT.
E21
Standard for Indoor 12kV Power-Electronic Fault-Limiting Circuit Breakers (EDS 03-6511)
E22
Standard for Indoor 12kV, 24kV and 36kV Metal Enclosed Switchgear for Grid and Primary Substations (EDS 03-6510)
E17
Equipment Reference Manual
C1A2
A systematic approach has been used to identify all reasonably foreseeable hazards that apply to the 'system' together with potential initiating events or sequences of events.
C1A2E1
A HAZID workshop was undertaken to identify hazards for the FLCB device in both the trials and general application.
C1A2E2
The HAZID was carried out by SQEP individuals.
E2
Powerful-CB HAZID Workshop Report (AMAT) (FNC 52680-46195R)
E1
Powerful-CB HAZID Workshop Briefing Note (FNC 52680-96871V)
E3
Powerful-CB Hazard Record (AMAT) (FNC 52680-98446V)
E2
Powerful-CB HAZID Workshop Report (AMAT) (FNC 52680-46195R)
C1A3
Methodology and evaluation criteria adopted for the risk assessment is clear and has been developed specifically for the use of AMAT FLCB devices on the electricity distribution network.
C1A3E1
The risk classification matric and acceptance criteria are documented and communicated to relevant stakeholders.
E5
Powerful-CB Safety Case Process and Principles (FNC 52680-45805R)
C1A4
A suitably sufficient and robust process has been undertaken to evaluate and assess the safety risks and identify reasonably practicable safety measures.
C1A4E1
A Risk Assessment Workshop was undertaken to assess risks of implementing the FLCB device on the network and to identify potential safety measures.
C1A4E2
RA Workshop was carried out by SQEP individuals.
E6
Powerful-CB Risk Assessment Workshop Report Issue 1 (FNC 52680-46624R)
E7
Powerful-CB Risk Assessment Workshop Briefing Document (FNC 52680-98714V)
E3
Powerful-CB Hazard Record (AMAT) (FNC 52680-98446V)
E6
Powerful-CB Risk Assessment Workshop Report Issue 1 (FNC 52680-46624R)
C1A5
Cost Benefit Analysis has been carried out, using recognised methodologies and robust data, to determine whether potential safety measures are necessary to ensure safety so far as is reasonably practicable.
C1A5E1
The input data used in the CBA is accurate and relevant.
C1A5E2
The CBA was conducted in accordance with recommended good practice.
E19
Powerful-CB Risk Assessment Workshop Report Issue 2 (FNC 52680-46624R)
E19
Powerful-CB Risk Assessment Workshop Report Issue 2 (FNC 52680-46624R)
E3
Powerful-CB Hazard Record (AMAT) (FNC 52680-98446V)
C1A6
Safety requirements have been derived from relevant applicable policies, procedures or regulations and the Risk Assessment.
C1A6E1
A HAZID Workshop was undertaken which derived the safety requirements.
C1A6E2
A Risk Assessment workshop and CBA was undertaken which derived the safety requirements.
C1A6E3
A Hazard Record has been developed which details the safety requirements.
E6
Powerful-CB HAZID Workshop Report (AMAT) (FNC 52680-46195R)
E19
Powerful-CB Risk Assessment Workshop Report Issue 2 (FNC 52680-46624R)
E3
Powerful-CB Hazard Record (AMAT) (FNC 52680-98446V)
C1A7
The outputs from all safety related activities are recorded and continually updated throughout the project.
C1A7E1
A Hazard Record has been developed and is continually updated throughout the project.
E3
Powerful-CB Hazard Record (AMAT) (FNC 52680-98446V)


Claim C2
The FLCB device is designed to operate effectively and safely for all postulated network fault conditions and satisfies the derived safety requirements.
C2N1
Verification of requirements are supported by FLCB Device manufacturers specification documents
C2A1
The FLCB device has been designed by competent designers to operate effectively and correctly.
C2A2
The designers have been integral to the safety assessment process and therefore have been able to inlfuence the design during the development.
C2A3
The FLCB device has been through testing and commissioned for use at the specified trial site.
C2A4
The FLCB device meets the legislative safety requirements.
C2A5
The design of the FLCB device satisfies the derived safety requirements.
C2A6
The data gathered during the trials will further substantiate the Safety Case
C2A1E1
Internal UKPN standards have been followed to ensure the device and associated equipment to be installed at the Grid and Primary substations operate effectively and correctly.
C2A1E2
AMAT FLCB Device Design Report presents the details of the device.
C2A1E1
Designers have attended the HAZID and RA Workshops and had an opportunity to review the outputs.
C2A3E1
Testing and Commissioning of the FLCB device has been completed to ensure it meets the functional and safety requirements.
C2A3E2
Reliability data and FMEA support the testing and commissioning of the device and trial site for safe implementation.
C2A4E1
Legislative compliance statements have been authored.
C2A4E1
The FLCB device meets the derived safety requirements.
C2A5E1
Trial Reports for the AMAT FLCB Device.
E21
Standard for Indoor 12kV Power-Electronic Fault-Limiting Circuit Breakers (EDS 03-6511)
E22
Standard for Indoor 12kV, 24kV and 36kV Metal Enclosed Switchgear for Grid and Primary Substations (EDS 03-6510)
E8
AMAT FLCB Device Design Report
E19
Powerful-CB Risk Assessment Workshop Report Issue 2 (FNC 52680-46624R)
E9
AMAT FLCB Testing and Commissioning Report
E20
The Reliability data and FMEA Report
E3
Powerful-CB Hazard Record (AMAT) (FNC 52680-98446V)
E3
Powerful-CB Hazard Record (AMAT) (FNC 52680-98446V)
E20
The Reliability data and FMEA Report
E10
Powerful-CB AMAT FLCB Trials Reports


C3N1
Safe means risk is Broadly Acceptable or Tolerable and ALARP.
Claim C3
The AMAT FLCB Devices can be implemented safely onto the electricity networks.
C3A1
A safe installation strategy has been developed for the trial.
C3A2
The commissioning activities verify that the FLCB devices have been installed in accordance with the strategy.
C3A3
Specific precautions are in place for the trial of the FLCB on the electricity network.
C3A4
There is sufficient resources to support the implementation of the FLCB Device for the trial and BAU.
C3A1E1
A Trial Installation Strategy Report has been produced.
C3A2E1
Installation and Commissioning Report has been produced.
C3A3E1
Installation strategy details the specific precautions to ensure fault current will not be exceeded.
C3A4E1
Resource plan for the implementation for the FLCB device for the trial and BAU has been produced.
E11
Trial Installation Strategy Report
E12
Network Installation and Commissioning Report
E11
Trial Installation Strategy Report
E13
Resource Plan for Trial and BAU


C4N1
Delivered includes design, install, operate, maintain, repair, decommission etc.
Claim C4
The safe operation of the FLCB's can be sustained throughout the trial, that the workforce is capable of delivering and assuring what is expected, and they are supported by accurate asset information.
C4N2
Workforce includes anyone, regardless of employer, working on or near power networks and sub-stations.
C4A1
The workforce is trained and competent to discharge their duties.
C4A2
Sufficient and appropriate resources are available to enable the workforce to discharge their duties.
C4A3
A fit for purpose assurance management system exists.
C4A4
The state of the infrastructure at any point in time is defined and available.
C4A2N1
Appropriate - resources are approved for use in the specific context.
C4A3N1
Assurance management using exiting Competence frameworks
C4A1E1
Training schedule and documents have been produced and competence management framework are in place to deliver a capable workforce.
C4A2E1
A Resource plan has been produced to ensure resource needs, requirements and appropriate tools are in place and available when required.
C4A3E1
Contractors operate robust assurance regimes that monitor and assess the performance of the implementation of the FLCB devices.
C4A4E1
Infrastructure reports are produced and any planned changes.
E14
Training and Competence Plan
E13
Resource Plan for Trial and BAU
E15
Assurance Management System Document
E16
Infrastructure Report

ANNEX B - SAFETY CASE EVIDENCE TABLE

The status of each piece of evidence is defined as:

- Green- A complete issued version of the evidence is held;
- Yellow – A draft version or a reference to the evidence is held;
- Orange – No evidence currently exists.

Table 1: Safety Case Evidence Table

ID	Reference	Document Title	Issue / Date	Status
E1	FNC 52680-96871V	Powerful-CB HAZID Workshop Briefing Note	Issue 1 June 2017	G
E2	FNC 52680-46195R	Powerful-CB HAZID Workshop Report (AMAT)	Issue 1 August 2017	G
E3	FNC 52680-98446V	Powerful-CB Hazard Record (AMAT)	Issue 2 April 2018	G
E4	-	Not Used	-	-
E5	FNC 52680-45804R	Powerful-CB Safety Case Process and Principles	Issue 1 May 2017	G
E6	FNC 52680-46624R	Powerful-CB Risk Assessment Workshop Report	Issue 1 November 2017	G
E7	FNC 52680-98714V	Powerful-CB Risk Assessment Workshop Briefing Document	Issue 1 September 2017	G
E8	TBC	AMAT FLCB Device Design Report	TBC	O
E9	TBC	AMAT FLCB Testing and Commissioning Report	TBC	O
E10	TBC	Powerful-CB AMAT FLCB Trial Reports	TBC	O
E11	TBC	Installation Strategy Report	TBC	O
E12	TBC	Network Installation and Commissioning Report	TBC	O
E13	TBC	Resource Plan for Trial and BAU	TBC	O
E14	TBC	Training and Competence Plan	TBC	O
E15	TBC	Assurance Management System Document	TBC	O
E16	TBC	Infrastructure Report	TBC	O

ID	Reference	Document Title	Issue / Date	Status
E17	TBC	AMAT FLCB Device Equipment Reference Manual	TBC	O
E18	HSS-01-051	UKPN Incident Reporting Procedure	Version 9.0 February 2018	G
E19	FNC 52680-46624R	Powerful-CB Risk Assessment Workshop Report	Issue 2 May 2017	G
E20	TBC	AMAT 250A FLCB Device Reliability Data and FMEA Report	TBC	O
E21	ETS 03-6511	Standard for Indoor 12kV Power-Electronic Fault-Limiting Circuit Breakers	Version 1.1 June 2017	G
E22	ETS 03-6510	Standard for Indoor 12kV, 24kV and 36kV Metal Enclosed Switchgear for Grid and Primary Substations	Version 5.0 August 2017	G

ANNEX C - FLCB DEVICE SPECIFICATION

Will include device description from AMATFLCB Device Equipment Reference Manual when issued.

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