ABS Consulting

Developing the Safety Case for ABB Surge Current Limiters

Prepared for
Electricity North West
by
ABS Consulting Ltd

Report N^{o}. 3166069/R/03
Issue 1
August 2014

DOCUMENT APPROVAL SHEET

Project N°: 3166069

Report N°: 3166069/R/03

Report Title: Developing the Safety Case for ABB Surge Current Limiters

Client: Electricity North West

Contact: Dr Geraldine Bryson

ISSUE	DATE	PREPARED	REVIEWED	APPROVED
Draft A	July 2014	NW MacLean (Principal Engineer)	P Hartley (Principal Engineer)	P Stewart (Director Nuclear Services)
Draft B	July 2014	P Hartley (Principal Engineer)	S Hole (Principal Engineer)	P Stewart (Director Nuclear Services)
Draft C	August 2014	P Hartley (Principal Engineer)	S Hole (Principal Engineer	P Stewart (Director Nuclear Services)
Issue 1	August 2014	[signature] P Hartley (Principal Engineer)	[signature] S Hole (Principal Engineer)	[signature] P Stewart (Director Nuclear Services)

DOCUMENT REVISION HISTORY

ISSUE	DESCRIPTION
Draft A	First issue for client comment.
Draft B	Updated with inclusion of FTA, and revised FMECA
Draft C	Amended in response to Client comments
Issue 1	Issued following comments.

DOCUMENT SUMMARY

The Is limiter device is a combination of a fast acting switch with high current carrying capability but low switching capacity and a fuse with high breaking capacity, mounted in parallel. When a short circuit is detected a small explosive charge in the main current carrying conductor is detonated. This ruptures the main current carrying path thus diverting the current to the fuse which quenches it. The entire operation takes place within a few milliseconds.

The principal reason for the fitting of an Is limiter is that as it will trip before the first peak of a short circuit current, switchgear and cabling downstream of the Is limiter will not be subject to the full fault current, and can either be of lighter construction, or of increased capacity.

There are, however, some existing concerns which are currently restricting the use of Is limiters. The Distribution Network Operators have a licence obligation to operate their networks in compliance with the Distribution Code, Department for Business, Innovation and Skills regulations and Health and Safety Legislation. The Distribution Network Operators have concerns about the use of these current limiting devices which are:

- The possibility that a failure of the current limiting device to operate could overstress switchgear.
- Any emerging legal liability for damage to equipment or consumers downstream of the Is limiters in the event of their incorrect operation.
- The lack of an associated ‘back up’ engineered system to prevent faults affecting downstream equipment.
- Their intrinsic safety.
- Functional testing.
- Their triggering integrity.

This document addresses these concerns and presents the arguments in a coherent logical and analytical format of a Safety Case. In particular the concern that the Is Limiter would fail to operate on demand is addressed and shown to be highly unlikely based on manufacturer’s data. This will allow a positive review by Regulator for the use of Is Limiters.

LIST OF ACRONYMS

ABB	ABB Group
ALARP	As Low As Reasonably Practicable
BERR	Department for Business Enterprise and Regulatory Reform (now Department for Business Innovation and Skills)
BIS	Department for Business, Innovation and Skills
DNO	Distribution Network Operator
DTI	Department for Trade and Industry (now Department for Business, Innovation and Skills)
ENW	Electricity North West
FMEA	Failure Mode and Effect Analysis
FMECA	Failure Modes, Effects and Criticality Analysis
HSE	Health and Safety Executive
HAZID	Hazard Identification
HAZOP	Hazard and Operability Study
ms	Milli Seconds
OFGEM	Office of Gas and Electricity Markets

CONTENTS

1 INTRODUCTION

1.1 Brief Description of the Operation of the ABB Is Limiter

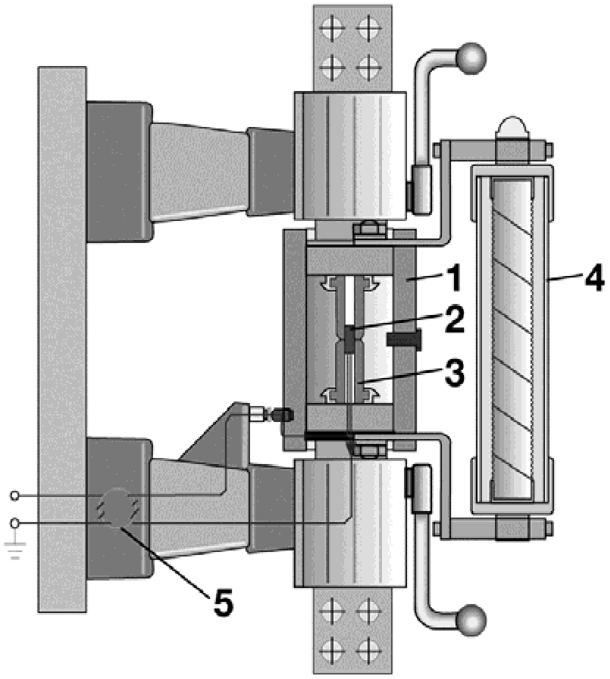


Figure 1 – Insert Holder and Insert

1 Insulating tube

2 Charge

3 Bursting Bridge

4 Fuse

5 Insulator with pulse transformer

The Is limiter device is a combination of a fast acting switch with high current carrying capability but low switching capacity and a fuse with high breaking capacity, mounted in parallel. When a short circuit is detected a small explosive charge in the main current carrying conductor is detonated. This ruptures the main current carrying path thus diverting the current to the fuse which quenches it. The entire operation takes place within a few milliseconds.

A small explosive charge is employed to give fast operation of the switch on the main conductor. Once the switch has operated, the current is diverted to flow in the parallel fuse where it is interrupted.

The current flowing through the device is monitored in an electronic measuring and tripping unit which is responsible for initiating the trip when an abnormally high and fast rising current is detected. Both magnitude and rate of rise of the current are monitored and tripping is initiated only when both quantities are above certain set values. The threshold magnitude and rate of rise of current can be set to suit the individual application.

For three-phase applications, the Is-limiter comprises three single pole holders with replaceable inserts, three tripping current transformers and one electronic measuring and tripping unit.

After operation the devices are isolated and the inserts containing the fuses and the ruptured conductors are removed and replaced with spares. A circuit breaker is always required in series with the Is Limiter, in order to perform normal circuit opening and closing duties.

1.2 Reasons for fitting the ABB Is Limiter

The principal reason for the fitting of an Is limiter is that since it will trip before the first peak of a short circuit current, based on the rate of rise of the current flow, switchgear and cabling downstream of the Is limiter could be of lighter construction. Alternatively, the use of Is limiters would allow existing cabling and switchgear to have a potentially higher rating, since the peak short circuit current will not be seen.

In these circumstances, conventional circuit-breakers cannot provide protection against high peak short-circuit currents, as they will not trip before the first peak of short circuit current. The Is limiter is capable of detecting and limiting a short-circuit current at the first rise, i.e. in less than 1 ms. The maximum instantaneous current occurring remains well below the level of the peak short-circuit current.

The Is limiter also has uses in transformer or generator feeders, in switchgear sectioning and connected in parallel with reactors.

1.3 DNO Concerns

The Distribution Network Operators (DNOs) have a licence obligation to operate their networks in compliance with the Distribution Code, Department for Business Innovation and Skills (BIS) regulations and Health and Safety Legislation. The DNOs have concerns about the use of these current limiting devices. The issues that they are particularly concerned about are:-

- The possibility that a failure of the current limiting device to operate could overstress switchgear.
- Any emerging legal liability for damage to equipment or consumers downstream of the Is limiters in the event of their incorrect operation.
- The lack of an associated ‘back up’ engineered system to prevent faults affecting downstream equipment.
- Their intrinsic safety.
- Functional testing.
- Their triggering integrity.

The Distribution Code of Licensed Distribution Network Operators (Reference 1), also contains rules which could make the use of Is limiters difficult.

DPC 4.4.4 (d) states:

> *Unless the DNO should advise otherwise, it is not acceptable for Users to limit the fault current in feed to the DNO’s Distribution System by the use of Protection and associated Equipment if the failure of that Protection and associated Equipment to operate as intended in the event of a fault, could cause Equipment owned by the DNO to operate outside its short-circuit rating.*

1.4 Work Already Conducted

Electricity North West commissioned ABS Consulting to investigate the feasibility of making a Safety Case to be able to use ABB Is Limiters within their Network. This was reported within ABS Report 3166069/R/01 (Reference 2).

This concluded that there are some minor administrative issues which would currently prevent the use of Is limiters:

- An Explosives Certificate or an exemption.
- Suitable maintenance procedures.
- Suitable training procedures for Operators and Maintainers.
- A risk assessment and training to enable the storage, transportation, fitting and operation of Is limiters.

It was considered that these issues would be relatively straightforward to overcome. To that end, they will not be discussed further within this report.

In addition, Reference 2 concluded that the principal barrier to the use of an Is limiter within a UK network would appear to be the consequences of the Is limiter failing to operate on demand. It was considered that the only way in which it would be possible to construct an adequate safety case would be to demonstrate that the likelihood of failure to operate on demand has been reduced to an acceptably low level. This report will demonstrate that the probability of failure on demand has been reduced to a level which is both tolerable and As Low As Reasonably Practicable (ALARP).

1.5 Introduction to a Safety Case

A safety case refers to the totality of a Duty Holder's documentation to demonstrate safety. It should consist of documentation to justify safety during the design, construction, manufacture, commissioning, operation and decommissioning phases of the installed equipment. A safety case (Reference 3) should present the following information appropriate to the complexity of the installation, the stage of the installation in its lifecycle and the scale and nature of the hazards on the installation:

A hazard identification technique, e.g.:

- Hazard Identification (HAZID),
- Hazard and operability study (HAZOP),
- Failure Modes and Effects Analysis (FMEA),
- Safety reviews,
- Industry standard or bespoke checklists,
- Job safety analysis.

A demonstration of sound engineering practice, e.g.:

- Derivation of operating limits,
- Examination, inspection, maintenance and testing regimes,
- Commissioning and trials information.
- Optimisation of protection and balanced plant design

Engineering Justification, e.g.:

- Inherent and passive safety,
- Codes and Standards,
- Redundancy and Diversity; Single Failure Criterion,
- High Integrity Design (with numerical targets),
- Consideration of Ageing and Degradation,
- Material Control,

Purpose and Limitations of Commissioning.

Design for Safety.

Consistency with function,

Safety Systems,

Monitoring and Control,

Role and Training of Operators.

It is considered that most of the information to establish a Safety Case already exists, or can be obtained without a substantial amount of additional work.

It was considered that it would be possible to construct an adequate safety case would be to demonstrate that the likelihood of failure to operate on demand has been reduced to an acceptably low level. This report will demonstrate that the probability of failure on demand has been reduced to a level which is both tolerable and ALARP.

2 HAZOP STUDY

A HAZOP Study was conducted for Electricity North West for the proposed implementation of current limiting devices to their electrical network, and reported in ABS Report 3166069/R/02 (Reference 4). The Study focused on the normal operation of the current limiting device concentrating on the effect potential failures/hazards had on safety of personnel and the commercial impact of equipment being damaged. The HAZOP Study was performed by a multi-disciplinary team made up of individuals from Electricity North West and ABB and facilitated by ABS Consulting. .

As part of the Hazard and Operability Study the following seven Nodes were considered:

- Node 1 - Current Transformers.
- Node 2 - Trip Inserts.
- Node 3 - Power Supply Unit.
- Node 4 - Trip Unit.
- Node 5 - Indication Unit.
- Node 6 - Circuit Breaker.
- Node 7 - Overall (general system hazard scenarios).

The output of the Study resulted in 6 recommendations being recorded within the HAZOP worksheets. The table below shows the distribution of the recommendations according to their risk ranking. The risk matrix was used to assess the severity and likelihood of all causes and consequences that were identified and examined. The use of the risk rankings will help to focus resources on the most significant risks.

Level 4	Level 3	Level 2	Level 1	Total
0	3	0	3	6

In summary, there were zero Level 4 recommendations identified with a risk ranking of Level 4 (High). There were three recommendations identified with a risk ranking of Level 3 (Medium), zero recommendations with a risk ranking of Level 2 (Medium-Low) and three recommendations with a risk ranking of Level 1 (Low). These are detailed overleaf.

The most prominent hazard identified with a risk ranking of Level 3 (Medium) was the loss of network electrical supply caused by the Is-limiter tripping. The potential consequence of this would be a loss of supply to customers for the duration it took to replace the trip inserts. This is a commercial issue, and not related to safety in any way. The recommendations proposed were to ensure the network was designed to safeguard that supply can be restored as quickly as possible, ensure adequate spare trip inserts are available and to ensure procedures and training are in place to replace trip inserts as quickly and safely as possible. If the recommendations are implemented, then the risk should be reduced to a level that is As Low As Reasonably Practicable (ALARP).

All of the recommendations from the HAZOP Study will now need to be monitored by Electricity North West and then closed out. Those who are allocated Study recommendation(s)/action(s) shall be responsible to close-out their actions. Actions should not be considered closed unless descriptions are accompanied by suitable and sufficient evidence.

Recommendations	Place(s) Used	Responsibility	Risk Ranking	Date Completed	Notes
1. Consider installation of UPS	Causes: 3.2.1	ENW	1		Over voltage Potential fault on LV Cable for auxiliary supply
2. Consider alarm function	Causes: 3.3.1	ENW/ABB	1		Under voltage Potential fault on LV Cable for auxiliary supply
3. Operational procedures put in place to check Is limiter following restoration of fault	Causes: 4.6.1, 4.6.2, 5.2.1	ENW	1		No Data or Control Signals
4. Correct network design to ensure that supplies can be restored as quickly as possible	Causes: 7.5.1	ENW	3		Loss of supply Is limiter trips Potential loss of supply to customers for length of time to replace inserts
5. Ensure procedures and training are in place to replace inserts	Causes: 7.5.1	ENW	3		
6. Make sure adequate spare inserts are available	Causes: 7.5.1	ENW	3		

Table 1 – HAZOP Recommendations

Overall, there were no safety concerns relating to the implementation of the Is-limiter. There are three independent phases, with only one phase required to operate at any giving time to provide protection to the network. In conclusion, the Is-limiter is functionally safe to implement to the Electricity North West electrical network.

3 FAILURE MODES, EFFECT AND CRITICALITY ANALYSIS

The section of this report uses the FMECA technique to identify any single line component failures. A single line failure for the purpose of this analysis is defined as:

> "Any component of the Is limiter devoid of redundancy and/or auxiliary devices whose failure would result in a short circuit current causing damage to equipment downstream of the Is limiter."

3.1 Scope

Within the scope of work assigned, there are two main requirements:

- Review the design of the Is Limiter to identify critical components and whether any single line component failures exist.
- Where such components are identified, carry out a review to recommend the practicability of any modifications that will result in their elimination. It should be noted that only failures which were likely to cause the Is limiter to fail to operate on demand were considered.

3.2 Methodology

The FMECA has been performed using the guidance laid down in BS EN 60812:2006, (Reference 5). Component level failure modes analysis is generally considered to be a 'bottom up' process which provides the opportunity for a number of differing failure modes to be assessed. To this end, basic Fault Trees were modelled which adopted a 'top down' approach. See Section 4

3.3 Assumptions

The following assumptions have been made with regard to this report:

- The aim of the FMECA is to determine single line component failures which would prevent the Is limiter operating on demand.

3.4 FMECA Definitions

The following definitions used in this report and supporting worksheets:

- Component: Any functional part of the system which can be individually considered. In the case of an assembly, this may be broken down further.
- Failure: Termination of the ability of the component to perform a required function.
- Failure Effect: Consequence of a failure mode in terms of the operation, function or status of the component.
- Failure Mode: Manner in which a component fails.
- System: A set of interrelating or interacting elements.
- Revealed Failure: A failure detectable during normal operation or maintenance.
- Hidden Failure: A failure not detectable during normal operation or maintenance. This is especially relevant for this analysis as non-redundant failure mechanisms have been examined.
- ALARP: Where a risk is reduced to a tolerable level and it can be demonstrated that the cost of reducing the risk further would be grossly disproportionate to the benefit gained.

3.5 Failure Modes

Due to the nature of the analysis, in that the aim is to determine single line component failures which would prevent the Is limiter operating on demand, not all of the failure modes shown in Reference 5 are relevant. For example, intermittent failures have not been considered as although these may have an impact, they would not ultimately lead to a catastrophic failure if addressed and rectified.

3.6 Components

The analysis has been broken down to capture the failure modes surrounding the following six components and assemblies:

- Current Transformer.
- Trip Inserts.
- Power Supply Unit.
- Trip Unit.
- Indication Unit.
- Circuit breaker.
- di/dt settings in trip unit

3.7 FMECA Worksheets

The FMECA tables are contained within Appendix A. Each assembly, as stated in Section 3.4, has been analysed and assigned a score to assess the criticality of each postulated failure. The scoring criteria are based on a semi-quantitative scale for severity, probability of occurrence and detectability for each failure. To keep the analysis as simple as possible and avoid subjective decision making between marginal scores, each scale is ranked from 1 to 5. The criticality is then calculated by multiplying all three scores together and determining acceptability of the outcome as follows:

Criticality Index	
Score < 15	No further mitigation required but should be reviewed periodically.
Score 15 to 24	Further mitigation should be investigated to provide an ALARP solution.
Score > 24	Additional mitigation must be applied to reduce the risk to a tolerable level.

Table 2 – Criticality Index

3.7.1 Output from FMECA Worksheets

The criticality score for all components are 1 or 3.

- There are no hardware components that could prevent the operation from failing to operate on demand. As the Is Limiter is an additional safety component, the normal function of the circuit breaker will provide protection to the circuit. It is acknowledged that the Peak current may result in stress damage to downstream equipment.

- In the event of the loss of the power supply either due to loss of Main or auxiliary power, or failure of the PSU itself, the unit will not operate. The power supplies are assumed to be provided from other sources with separate alarms. To provide added integrity it is recommended that an UPS should be installed at this point.
- The system relies on the setting of the di/dt value using variable resistance in an RC circuit. This is a potential weakness as it relies on an operator to establish the desired rate of change characteristic (di/dt) for the specific circuit loading. A second operator is required to input and test this value correctly.

4 FAULT TREE

4.1 Structure

A simple fault tree was constructed. See Appendix B. The basic block diagram provided in the ABB literature was used.

4.2 Reliability data

Failure rate data was extracted from the Nonelectronic Parts Reliability Data 2011. This data base is produced by the US Defense Systems Information Analysis Center (formerly Reliability Information Analysis Center RAIC). This is a widely used reliability database.

The component title and source page of the data is included in the fault tree for completeness.

4.3 Discussion

It is not possible to carry out a calculation to assess the probability of failure on demand and equate with either those published in 2004 by DTI (Reference 3) or TŰV Rheinland in 2007 (Reference 7) . To do this, access would be required to both their models and data sets. Updated models could then be created and validated, and an assessment could then be made using more up to date data.

5 SAFETY CASE DISCUSSION

5.1 Introduction

A safety case refers to the totality of a Duty Holder's documentation to demonstrate safety. It should consist of documentation to justify safety during the design, construction, manufacture, commissioning, operation and decommissioning phases of the installed equipment. A safety case should present the following information:

- A hazard identification technique appropriate to the complexity of the installation, the stage of the installation in its lifecycle and the scale and nature of the hazards on the installation.
- A demonstration of sound engineering practice.
- Engineering Justification.
- Design Basis Analysis.
- Design for Safety.
- Role and Training of Operators.

5.2 Hazard Identification

A failure modes and criticality effects analysis has been conducted which shows that there are no critical components that can prevent the system operating as designed.

5.3 Sound engineering practice

The design of the Is limiter relies on components using proven technology. It is acknowledged that the use of a small explosive charge in the bursting bridge is novel to the electricity supply industry. However, the use of similar devices in large numbers in modern cars as a proven safety feature with a record of reducing personal injuries suggests that this is now acceptable technology. Reference 1 contains a description of the handling, transport and storage arrangements required for the explosive charges.

5.4 Engineering Justification

5.4.1 Testing regime of the Is limiter charge elements

As discussed in Reference 1 and elsewhere in this report, there is no way to actually test the tripping mechanism. It is possible to test the triggering circuitry, and the manufacturers have a maintenance procedure for this, but the operation of the actual tripping device (i.e. the pyrotechnic charge) cannot be tested. This is not an unusual situation, for example, mechanical systems that use Bursting Discs to release pressure have a similar disadvantages, which this report will draw a comparison with – there is no way to be absolutely certain that the device will operate when it is required.

The manufacturers of the charge element carry out extensive testing of each batch of charges that they manufacture. Information from ABB indicates that the following testing is carried out (Note: For information, the batch of charges described by ABB is of 2000 charge units):

Visual checks and Measurements are carried out on 100% of the charge elements.

Visual checks:

- No holes and cracks in the charge.
- Sealing of the charge cover. No explosive material has trickled out of the charge-housing, no adherence of pyrotechnic material "dust".

- No visible foreign material, no blow holes, no defects on edges of charge, no peeling of material.
- No visible contamination/pollution.
- No visible corrosion.

Measurement:

- Dimensions of the charge element (length, diameter).
- Inner electrical impedance.

Function of the charge (i.e. activation of the charge)

- 5 % of the charges are activated at 35°C.
- 5 % of the charges are activated at standard environmental conditions.
- 5% of the charges are activated at 60 °C.

In total 15% of the charge elements in each batch will be triggered during the internal test procedures of the charge sub-supplier. The manufacturer has no record of failures.

> Note: Merely to provide a comparison, a comparable mechanical safety device that can only be tested destructively is a bursting disc. For batches of the size of the trip insert charges, a maximum of 3% of the bursting discs require to be destructively tested Reference 6.

The trip inserts have a manufacturer's recommended service life. Inserts that are returned are tripped. The manufacturer has no record of any returned inserts failing to trip on demand.

The manufacturer also has no record of an in service Is limiter failing to trip on demand.

5.4.2 Comparable Mechanical System testing

Reference 6 states that the destructive testing for bursting discs should be as follows:

Total number in a batch	**Number to be tested**
Less than 10	2
10 to 15	3
16 to 30	4
31 to 100	6
101 to 250	4 % but not less than 6
251 to 999	3 % but not less than 10
1 000 and greater	Minimum 30

Table 3 — Number of bursting discs to be tested

It can be seen from the table above that even using the most favourable statistics for bursting disc testing, the proportion of Is limiter charge elements that are destructively tested is at least comparable. For large batch sizes, the proportion of Is limiter charge elements is at least five times greater than for bursting discs.

5.5 Design for Safety.

Design for safety comprises three aspects:

1. Consistency with function. The Is Limiter is designed for one function alone, and has no other interface that could comprise its primary, and only, function.

2. Safety Systems.

- As a standalone device, the Is Limiter does not rely on the operation of another component of the power distribution network for its operation. It is a standalone device that contributes to the overall defence in depth. Note: The circuit breaker alone requires an integral power supply unit for its operation.
- With one Is Limiter on each phase, only one is required to actuate to isolate the supply at the circuit breaker: in effect there is redundancy for this safety mechanism for phase to phase faults.

3. Monitoring and Control. The Is limiter is self-contained. Monitoring is either by routine maintenance, or replacement of ruptured conductors.

5.6 Role and Training of Operators.

The Is limiter is not new technology, they have been in service worldwide for many years. The manufacturer has developed a set of maintenance and inspection procedures, as well as bespoke testing equipment to check the correct operation of the Is limiter.

It would be for ENW to demonstrate that they had a sufficient number of persons trained to competently conduct maintenance and testing on the Is limiter. It is not considered that this would present an issue.

5.7 Failure on Demand

Some of the regulations discussed earlier place absolute requirements on the network operators, rather than requirements which are to be complied with 'so far as is reasonably practicable'. One of these absolute requirements is that the equipment used in the network must be fit for purpose, i.e. it must sufficiently robust to be able to withstand a potential short circuit current. Surge limiters offer the advantage that since they are designed to operate before the first peak of any short circuit, the network will not see those peak current, so that there is the potential to utilise cabling and switchgear of a lesser capacity. This of course offers a potential to make substantial cost savings, but cost saving alone cannot be used as a justification for changes to a network. It is generally understood that for cost saving to be a factor, the overall risk should not be significantly greater than it was before.

To complicate matters, there is no way to actually test the tripping mechanism. It is possible to test the triggering circuitry, and the manufacturers have a maintenance procedure for this, but the operation of the actual tripping device (i.e. the pyrotechnic charge) cannot be tested. This is not an unusual situation, mechanical systems that use Bursting Discs to release pressure have a similar disadvantage, as do Airbag ignition in cars – there is no way to be absolutely certain that the device will operate when it is required.

5.8 Current Mitigation

There are several current mitigating factors.

- Operational experience.
- Redundancy.
- Existing safety studies.
- Trip units taken out of service.
- Changes in Legislation.

These are discussed below.

5.8.1 Operational Experience

There is considerable operational experience in the use of Is limiters world-wide. The Is limiter has been in service since 1961. Reference 7 indicates in excess of 120,000 device years of operation. In that time, ABB have no record of the Is-limiter device failing to operate on demand.

There have been five cases of spurious trips. Investigation showed that all five cases were related to a change in the network by the operators, who had installed capacitor banks without checking the settings of the existing Is-limiters. The charging and discharging of these capacitor banks, and the resulting high rate of rise, high peak currents had caused the Is-limiter to trip. ABB have no record of injury to people arising from hazardous incidents associated with the transport, storage, operation, maintenance and disposal of the Is-limiter units.

Therefore, since Reference 3 was produced in 2004, a 'proven in use' argument can be made based on the last 10 years years of successful operation.

5.8.2 Redundancy

The system is to be installed in 3 phase installations. There are 3 possible fault scenarios:

- Phase to phase short circuit
- Single Phase to ground: the Electricity North West network is operated with a resistance earth. Therefore the "ground" fault current is limited by the resistance.
- All phases to ground: as single phase

For all faults involving more than one phase the Is-Limiter construction offers redundancy in that each phase is completely independent and only one phase is required to operate to interrupt the current.

5.8.3 Existing Safety Studies

ABB commissioned TŰV Rheinland to conduct an assessment of the safety related reliability of the Is Limiter. TŰV Rheinland published a Report – Report Number 968/EL 444.00/07 Report on the determination of the safety related reliability of the Is limiter type BA 323/04 E, dated 2007-01-03 (Reference 7).

The scope of the report was to conduct a Failure Mode and Effects Analysis (FMEA) on the components of the Is limiter, and to calculate the safety parameters according to IEC 61508 (Reference 8).

The outcome of the study was that the average probability of failure on demand (per year) was calculated as:

One Phase System – 4.9×10^{-5}.

Three Phase system – 1.02×10^{-4}.

These results are more optimistic that those published in 2004 by DTI/Parsons Brinkerhof (Reference 3). Given seven more years of incident free operational data since the TŰV Rheinland report, and an increasing number of the devices in use, it may be possible to suggest an improvement of a further decade in the probability of failure on demand. This can only be validated by updating the TŰV Rheinland assessment model.

5.8.4 Trip Units taken out of Service

The tripping inserts have a recommended in service life – either 8 years in service, or 12 years if they have not been connected. This service life is dictated by the bursting charge component.

The inserts are returned to the manufacturer, where they are then tripped, to check their correct operation. Information from ABB indicates that they refurbish between 450 and 600 of these inserts per year. ABB do not keep data from individual tests, but they report that this is because they have had no instances of the inserts failing to operate when destructively tested in this fashion.

5.8.5 Changes in Legislation.

A review of the HSE website suggests the following issued and updated documents since 2004:

- Memorandum of guidance on the Electricity at Work Regulations 1989 Guidance on Regulations updated 2007. Regulation 11 'Means for protecting from excess of current'. This recognises the wide range of protective equipment circuits and environments in which they will be used and allows for a reasonable argument to be made to permit their use in specific situations.
- Electricity at work: Safe working practices (2013). Provides advice on safe working practices for managers and supervisors who control or influence the design, specification, selection, installation, commissioning, maintenance or operation of electrical equipment.
- The following standards have been updated that are pertinent to the use of current limiters:
    - BS 6626: 2010. Code of practice for maintenance of electrical switchgear and control gear for voltages above l kV and up to and including 36 kV
    - BS 7671: 2008 – 2011. Requirements for electrical installations. IEE Wiring Regulations. Seventeenth edition

- BS EN 50110 Parts 1 and 2 2004 – 2010. Operation of electrical installations

5.9 Safety Case Summary

The potential advantage of an Is limiter is that because it interrupts the surge current from a short circuit before it reaches its peak, the downstream circuitry never sees the full surge current, therefore it need not be of such a high capacity.

The principal issue with the Is limiter is one of being able to demonstrate reliability. Should the Is limiter operate as designed, then there is no reason that would prevent their use in a network in the UK. However, Reference 1 is quite clear that should the Is limiter fail to operate, and equipment downstream was overstressed, the network operator would be in breach of current legislation. It should be noted that this would only apply if the Is limiter was fitted in conjunction with cabling and switchgear that could be overstressed.

To satisfy an absolute requirement of any of the legislation, the integrity levels as they currently stand would not be suitably robust enough to provide an argument that the probability of failure on demand is not credible. There is also some ambiguity between the available operational data and the reliability figures published in Reference 4 and Reference 7. Although a definitive figure of accepted reliability is not available for this application, in the nuclear industry, a probability of failure on demand of the order of $1x10^{-6}$ would be required. Given that level of reliability, a lesser, and pessimistic figure of $4.9x10^{-5}$ failure on demand (per year) is considered acceptable.

6 FINDINGS/CONCLUSIONS

As can be seen from the comments in previous sections, there are no safety concerns with the proposed use of Is limiters in a UK network. There are 5 issues which require to be addressed so that an Is limiter could be used within a network.

1. An Explosives Certificate (one required for each Local Authority in whose area one of these Is limiters is installed).
2. Suitable maintenance procedures. Those developed by the manufactures should if compliant with EU directives be suitable for use after a review. Maintenance procedures should also include procedures to inspect for damage in the event of a suspected failure on demand, i.e. overstress of down-stream components.
3. A suitable risk assessment and training to enable the storage, transportation, fitting and operation of Is limiters.
4. The assessment is that the Is limiter has the required reliability in service, and that the probability of failure on demand is at a very low level.
5. A positive opinion from HSE/Ofgem for the proposed use of Is Limiters.

7 RECOMMENDATIONS

It is considered that the Is limiter is appropriate for use in the UK, based on its assessed reliability performance on demand and its current use in Europe. The risks are that in the failure to operate on demand, the down-stream equipment may be damaged. Loss of life associated with this is unlikely as the down-stream equipment will be in its normal operating state with all protective features in place.

There are also administrative aspects to be resolved, as listed in section 5, before to a full safety case can be prepared for regulatory review by Ofgem and HSE.

8 REFERENCES

1. The Distribution Code of Licensed Distribution Network Operators of Great Britain: Issue 22:February 2014.

2. ABS Report 3166069/R/01 Feasibility of a Safety Case for ABB Surge Limiters dated April 2014.

3. DTI Report Number: URN 04/1066 Development of a safety case for the use of current limiting devices to manage short circuit currents on electrical distribution networks. Contract Number DG/CG/00022/00/00.

4. ABS Report 3166069/R/02 Hazard And Operability Study Report ABB current limiting device dated 19 May 2014.

5. BS EN 60812:2006, 'Analysis techniques for system reliability – Procedure for failure modes and effects analysis (FMEA), May 2006.

6. ISO 4126-2:2003 Safety devices for protection against excessive pressure — Part 2: Bursting disc safety devices.

7. TŰV Rheinland Report Number 968/EL 444.00/07 Report on the determination of the safety related reliability of the Is limiter type BA 323/04 E, dated 2007-01-03.

8. IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems.

Appendix A

FMECA tables

FMECA Worksheet 1																	
Project No: 3166069 **Project Manager:** N MacLean		**Mode of operation:** Normal		**Date of Assessment:** May 2014						**Analyst:** N MacLean **Checked By:** P Stewart							
		Component: Is limiter Current Transformer		**Function(s):** To provide current indication to the trip unit.													
						Actual					**Proposed**						
Ref	**Failure Mode**	**Failure Effects**	**Failure cause**	**Visibility to Operator**	**Single Line Y/N**	**Current Mitigation**	**P**	**S**	**D**	**Crit Index**	**Proposed Mitigation**	**Complete (Date)**	**P**	**S**	**D**	**Crit Index**	**Notes**
1.1	CT does not supply trip signal to trip unit.	Trip unit does not trip on short circuit.	Open circuit on cabling from CT to trip unit. Failure of CT.	No	N	3 independent phases. Maintenance and inspection procedures.	1	1	1	1	No further proposed mitigation.						

FMECA Worksheet 2																		
Project No: 3166069 **Project Manager:** N MacLean		**Mode of operation:** Normal		**Date of Assessment:** May 2014							**Analyst:** N MacLean **Checked By:** P Stewart							
		Component: Is limiter Trip Inserts		**Function(s):** To disrupt the circuit on receipt of a trip signal from the trip unit when both threshold current, and rate of change exceed the set values.														
						Actual					**Proposed**							
Ref	**Failure Mode**	**Failure Effects**	**Failure cause**	**Visibility to Operator**	**Single Line Y/N**	**Current Mitigation**	**P**	**S**	**D**	**Crit Index**	**Proposed Mitigation**	**Complete (Date)**	**P**	**S**	**D**	**Crit Index**	**Notes**
2.1	Trip Insert does not operate on demand.	Is limiter does not trip on short circuit, potential damage to downstream circuits.	Failure of Trip Insert (manufacturing fault). Ageing of charge. Broken Connection.	No	N	3 independent phases. Inspection procedures during and after manufacture. Testing of 15% of each batch post manufacture. Recommended service life. Testing of inserts after they are withdrawn from service.	1	1	1	1	No further proposed mitigation						

FMECA Worksheet 3																		
Project No: 3166069 **Project Manager:** N MacLean		**Mode of operation:** Normal		**Date of Assessment:** May 2014							**Analyst:** N MacLean **Checked By:** P Stewart							
		Component: IS limiter Power Supply Unit		**Function(s):** To provide power to the trip unit.														
						Actual					**Proposed**							
Ref	**Failure Mode**	**Failure Effects**	**Failure cause**	**Visibility to Operator**	**Single Line Y/N**	**Current Mitigation**	**P**	**S**	**D**	**Crit Index**	**Proposed Mitigation**	**Complete (Date)**	**P**	**S**	**D**	**Crit Index**	**Notes**	
3.1	No power output to Trip Unit	Trip unit fails to operate	1. Loss of Main power 2. Loss of Aux Power 3. Failure of PSU	Alarms	N	3 independent phases. Maintenance and Inspection procedures. Self-monitoring system. Alarm function.	1	2	1	2	Use of an Uninterruptable Power supply							

FMECA Worksheet 4																		
Project No: 3166069 **Project Manager:** N MacLean		**Mode of operation:** Normal		**Date of Assessment:** May 2014							**Analyst:** N MacLean **Checked By:** P Stewart							
		Component: Is Limiter Trip Unit		**Function(s):** To provide current indication to the trip unit. di/dt setting input														
						Actual					**Proposed**							
Ref	**Failure Mode**	**Failure Effects**	**Failure cause**	**Visibility to Operator**	**Single Line Y/N**	**Current Mitigation**	**P**	**S**	**D**	**Crit Index**	**Proposed Mitigation**	**Complete (Date)**	**P**	**S**	**D**	**Crit Index**	**Notes**
4.1	Trip Unit fails to send trip signal to trip insert. Insert does not operate on demand.	Is limiter does not trip on short circuit, potential damage to downstream circuits.	Failure of Current Transformer (see above.) Failure of capacitor in trip unit. Broken Connection.	No	N	3 independent phases. Maintenance and Inspection procedures. Self-monitoring system. Alarm function.	1	1	1	1	No further proposed mitigation.						
4.2	Trip unit activates too late.	Is limiter trips too late on short circuit, potential damage to downstream circuits.	Incorrect di/dt settings applied to trip unit.	No	Y	Maintenance and Inspection procedures.	1	1	1	1	No further proposed mitigation.						

FMECA Worksheet 5

Project No: 3166069
Project Manager: N MacLean

Mode of operation: Normal

Date of Assessment: May 2014

Analyst: N MacLean
Checked By: P Stewart

Component: Is limiter Indication Unit

Function(s): To display Is Limiter status and Alarm information to the operator.

						Actual					Proposed						
Ref	**Failure Mode**	**Failure Effects**	**Failure cause**	**Visibility to Operator**	**Single Line Y/N**	**Current Mitigation**	**P**	**S**	**D**	**Crit Index**	**Proposed Mitigation**	**Complete (Date)**	**P**	**S**	**D**	**Crit Index**	**Notes**
5.1	No Failure modes which could prevent the Is limiter from operating on demand.										No further proposed mitigation.						

FMECA Worksheet 6																	
Project No: 3166069 **Project Manager:** N MacLean		**Mode of operation:** Normal		**Date of Assessment:** May 2014							**Analyst:** N MacLean **Checked By:** P Stewart						
		Component: Is limiter series Circuit Breaker		**Function(s):** Circuit Breaker													
						Actual					**Proposed**						
Ref	**Failure Mode**	**Failure Effects**	**Failure cause**	**Visibility to Operator**	**Single Line Y/N**	**Current Mitigation**	**P**	**S**	**D**	**Crit Index**	**Proposed Mitigation**	**Complete (Date)**	**P**	**S**	**D**	**Crit Index**	**Notes**
6.1	No Failure modes which could prevent the Is limiter from operating on demand.										No further proposed mitigation.						

FMECA Worksheet 7

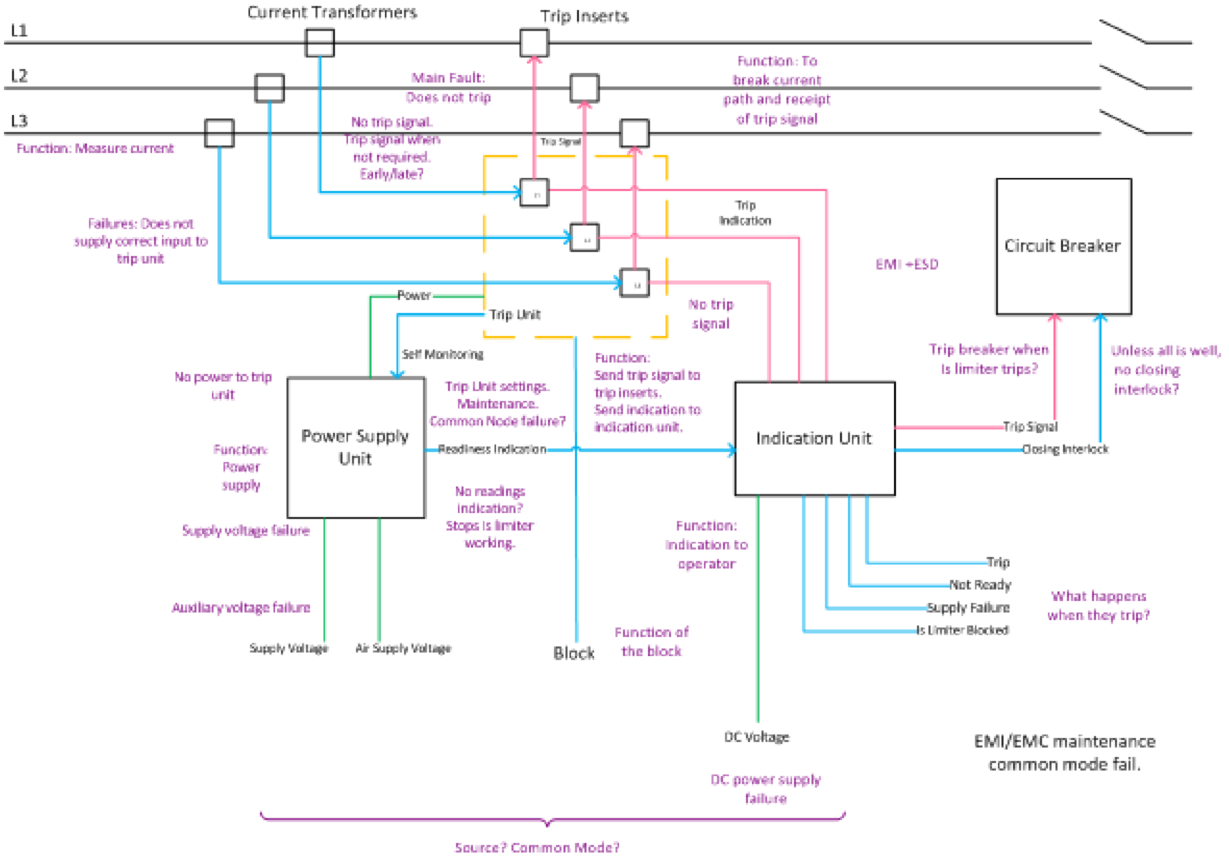
Project No: 3166069 **Project Manager:** N MacLean	**Mode of operation:** Normal	**Date of Assessment:** May 2014	**Analyst:** N MacLean **Checked By:** P Stewart
	Component: Tripping Unit di/dt settings(housed within Tripping Unit)	**Function(s):** To detect fault current increase	

						Actual					**Proposed**						
Ref	**Failure Mode**	**Failure Effects**	**Failure cause**	**Visibility to Operator**	**Single Line Y/N**	**Current Mitigation**	**P**	**S**	**D**	**Crit Index**	**Proposed Mitigation**	**Complete (Date)**	**P**	**S**	**D**	**Crit Index**	**Notes**
7.1	Settings incorrectly calculated for the circuit.	Trip unit does not trip on short circuit.	di/dt value too high for design fault current.	No	N	Testing procedures during installation. Maintenance and inspection procedures	1	1	1	1	No further proposed mitigation.						

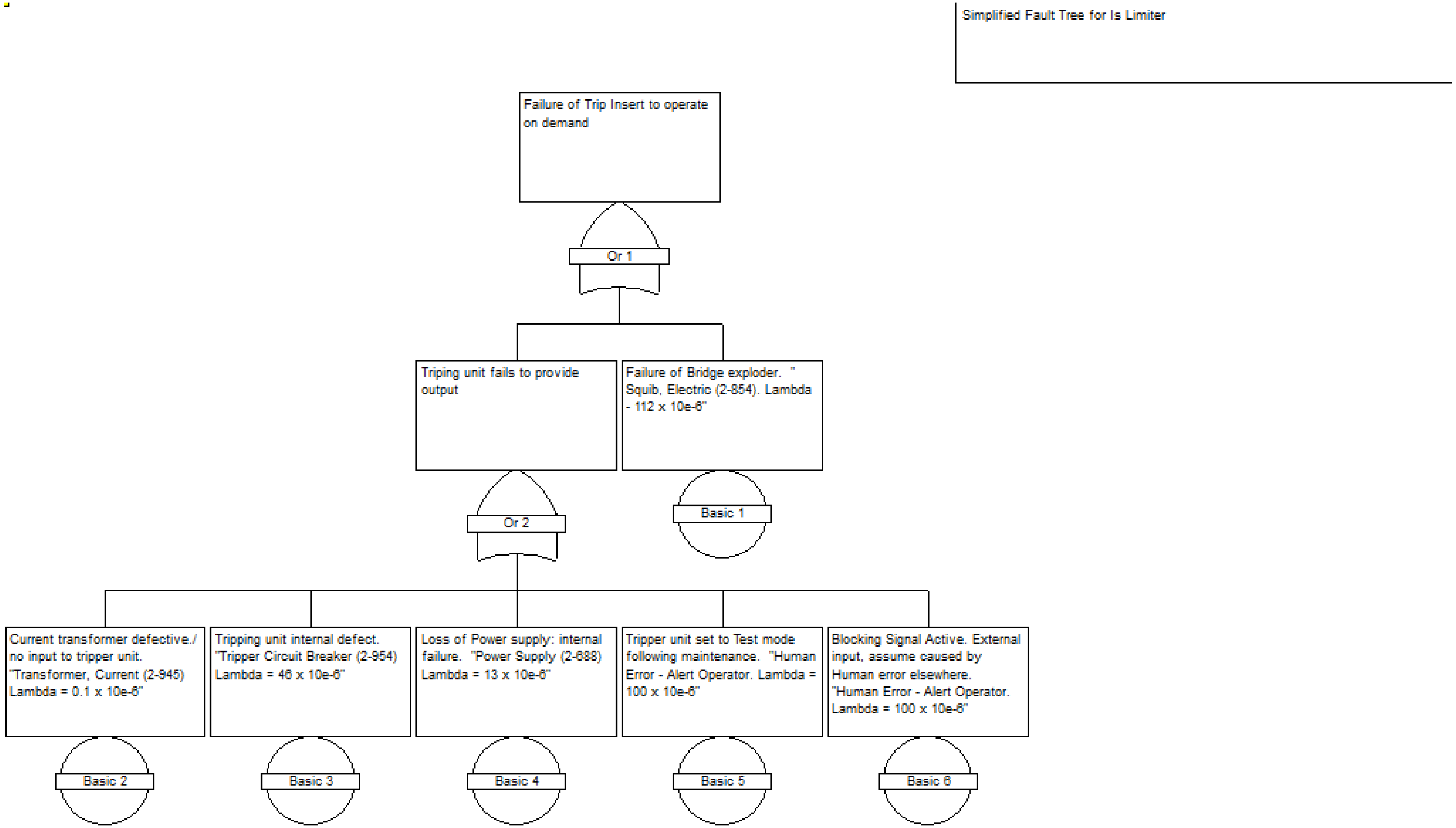
Appendix B

Fault Tree

System block Diagram



Fault tree


Simplified Fault Tree for Is Limiter
Failure of Trip Insert to operate on demand
Or 1
Triping unit fails to provide output
Failure of Bridge exploder. " Squib, Electric (2-854). Lambda - 112 x 10e-6"
Or 2
Basic 1
Current transformer defective./ no input to tripper unit. "Transformer, Current (2-945) Lambda = 0.1 x 10e-6"
Tripping unit internal defect. "Tripper Circuit Breaker (2-954) Lambda = 46 x 10e-6"
Loss of Power supply: internal failure. "Power Supply (2-688) Lambda = 13 x 10e-6"
Tripper unit set to Test mode following maintenance. "Human Error - Alert Operator. Lambda = 100 x 10e-6"
Blocking Signal Active. External input, assume caused by Human error elsewhere. "Human Error - Alert Operator. Lambda = 100 x 10e-6"
Basic 2
Basic 3
Basic 4
Basic 5
Basic 6

ORIGINATING OFFICE
ABS Consulting Ltd
Afton House,
26 West Nile Street,
Glasgow, UK, G1 2PF
Tel: +44 141 2046380, Fax: +44 141 2046399

CORPORATE HEADQUARTERS
ABSG Consulting Inc.
ABS Plaza, 16855 Northchase Drive
Houston, TX 77060
Tel: (281) 877-6100, Fax: (281) 877-6701
www.absconsulting.com

Offices Worldwide:

USA
Arlington, VA
Baltimore, MD
Houston, TX
Irvine, CA
Knoxville, TN
Lakewood, CO
Oakland, CA
Rockville, MD
St. Louis, MO
Salt Lake City, UT
San Antonio, TX
Seattle, WA
Stratham, NH
Wilmington, DE

Latin America
Caracas, Venezuela
Ciudad del Carmen, Mexico
Macaé, Brazil
Mexico City, Mexico
Monterrey, Mexico
Reynosa, Mexico
Rio de Janeiro, Brazil
São Paulo, Brazil
Veracruz, Mexico
Viña del Mar, Chile

Europe/Middle East
Aberdeen, UK
Abu Dhabi, UAE
Ahmadi, Kuwait
Bristol, UK
Dammam, Saudi Arabia
Derby, UK
Doha, Qatar
Dubai, UAE
Genoa, Italy
Glasgow, UK
Istanbul, Turkey
London, UK
Muscat, Oman
Paris, France
Piraeus, Greece
Rotterdam, The Netherlands
Sofia, Bulgaria
Vizcaya, Spain
Warrington, UK

Asia/Pacific
Bangkok, Thailand
Beijing, China
Jakarta, Indonesia
Kuala Lumpur, Malaysia
Manila, Philippines
Navi Mumbai, India
New Delhi, India
Pusan, Korea
Seoul, Korea
Shanghai, China
Singapore
Taiwan, China
Yokohama, Japan