CIRED 2020 Berlin Workshop (CIRED 2020)

22-23 September 2020

Theme 1: Integrating New Flexibility Tools and Principles for Planning

Pragmatic method for assessing the security of supply in future smart distribution networks

ISSN 2515-0855
doi: 10.1049/oap-cired.2021.0312
www.ietdl.org

David M. Greenwood[1] ✉, Predrag Djapic[2], Ilias Sarantakos[1], Spyros Giannelos[2], Goran Strbac[2], Alan Creighton[3]

[1]Newcastle University, UK
[2]Imperial College London, UK
[3]Northern Powergrid, UK
✉ *E-mail: david.greenwood@newcastle.ac.uk*

Abstract: Future distribution networks will be able to provide security of supply through a combination of conventional and smart solutions. This has the potential to require complex and time-consuming assessments using cost-benefit analysis and probabilistic, risk-based methods. The key goal of this project is to create a method for evaluating the security of supply from a combination of conventional and smart solutions which is rigorous enough to provide robust answers, but simple enough that it can be used routinely by planning engineers without in-depth knowledge of risk, statistics, probability, or reliability theory. This will be accomplished through an iterative, data-driven approach and validated via established risk analysis methods. This study presents underpinning analysis for the development of that method, including in-depth risk studies and sensitivity analysis of real distribution networks.

1 Introduction

Distribution network security has traditionally relied on conventional network assets such as transformers and circuits to ensure a secure supply to consumers from the upstream network. In recent years, there has been increasing interest in utilising smart solutions, including customer flexibility, to improve cost efficiency and increase the security of supply, because these solutions may already be connected to the network and may already be providing a *fortuitous contribution* to network security. In other cases, the distribution network operator (DNO) could contract with the operators of such solutions to explicitly provide network security when required by the DNO. The planning standard in Great Britain, Engineering Recommendation (EREC) P2/7 [1], is a deterministically applied, rule-based standard, focused on ensuring sufficient network redundancy is available to supply customers by specifying the times within which some or all customer demand during peak conditions should be restored. GB DNOs have a license obligation to plan and develop their systems so that it complies with the minimum requirements set out in this standard. The most recent version of this standard explicitly permits the security contribution from smart solutions to be considered alongside that from conventional network assets.

Current planning and operation paradigms of electrical distribution networks are facing fundamental challenges:

- Decarbonisation of the energy system is expected to drive large-scale electrification of transport and heat, which could lead to increased electricity demand and changes in the times of peak electricity consumption, both of which may trigger network reinforcement.
- Widespread deployment of low-carbon technologies, a large proportion of which will be connected to distribution networks, may increase stress on networks and introduce additional uncertainty to the demand. These technologies may provide a benefit, offsetting local demand and reducing the need for network reinforcement.

Options for network reinforcement using conventional assets and smart systems – such as distributed generation, flexible demand, energy storage systems, and advanced network technologies – to meet the required security standard in a cost-effective way are illustrated in Fig. 1. The case shows a demand of 30 MW, secured by two 30 MVA transformers, growing to 35 MW and requiring a system capacity increase.

This project aims to develop tools and methods to inform decisions about providing security of supply through a combination of conventional assets and smart solutions, creating a level playing field on which all solutions can compete equitably. A method that is intended for use by network design or planning engineers with no specialist training in risk analysis or probabilistic methods will be developed within the project. It will be validated using a sophisticated risk-based evaluation of the security of supply at real Northern Powergrid (NPg) substations using existing and predicted future demand profiles. The method will:

- Enable network design and planning engineers to evaluate the security contribution of one-or-more smart solutions without the need for specialist methods or knowledge;
- create a level playing field on which both network and smart solutions can be compared equitably; and
- provide transparency about the applicability of the method and its accuracy.

2 Risk evaluation methodology

The first step in producing a pragmatic method to assess the security of supply from conventional and smart solutions is to have a method for evaluating the risk in a given network; that method is described in this section.

2.1 Evaluating expected energy not supplied

Expected energy not supplied (EENS) is a widely used metric for network risk. Alternative terminologies are expected unserved energy, non-served energy, expected energy un-served, loss of energy expectation. EENS is calculated as the sum of products of

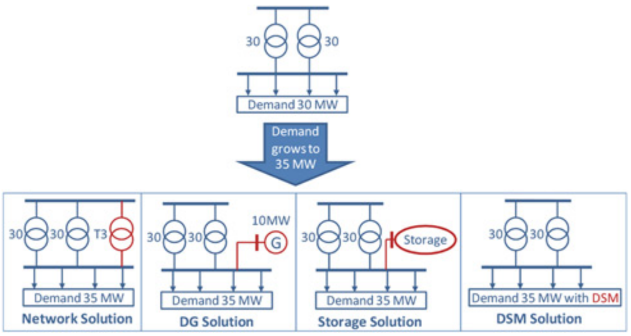

Fig. 1 *Range of network, including load transfer, and smart solutions for increasing supply security [2]*

the energy the system would be unable to deliver in a given state, and the probability of that state; mathematically this is

$$\text{EENS} = \sum_{i=1}^{N} p_i \cdot \text{ENS}_i \tag{1}$$

where ENS_i is the energy not supplied in a given state, p_i is the probability of that state occurring, and N is the total number of possible states the system could occupy.

In most real systems, N is too large to allow all the possible states to be enumerated; this is due to the number of combinations of possible outage states, and the variation of network demand – each of which is considered to be a separate outage state. In the method described, these issues have been dealt with in the following ways:

(i) Outages beyond the second circuit outage are considered to have a probability of occurrence that is too low to meaningfully impact the EENS. The results from the baseline risk analysis on the NPg networks show that the EENS arising from second circuit outage events are typically two orders of magnitude lower than those associated with first circuit outages, so it is reasonable to assume that the EENS arising from third circuit outage events will be negligible.
(ii) The time variation of network loads is represented using load duration curves (LDCs). This allows the variability of demand to be included without resulting in an intractable number of system states.

2.2 Risk arising from a first circuit outage

The following process is used to assess the EENS arising from a first circuit outage, or more specifically a first circuit fault (rather than a planned) outage:

(1) Segment each 11 kV feeder into discrete sections with an isolation point at each end.
(2) The expected annual unavailability, U_s, is the product of the probability of the system being intact, p_0 (which is close to 1), the failure rate, λ_s and the outage duration t_sl.
(3) The outage duration for each affected load is estimated using an automated algorithm in the model which analyses the options to restore supplies by switching without creating a thermal or voltage violation.
(4) Repairs are initiated to restore supplies to remaining customers. If any customers cannot be fully supplied, the average outage duration is the urgent repair time; otherwise, the non-urgent repair time is used.
(5) Once switching has been completed, the total demand of the customers supplied via each circuit can be established by summing the LDCs (i.e. a common LDC scaled by the peak demand of each load point) for each load supplied by that circuit.

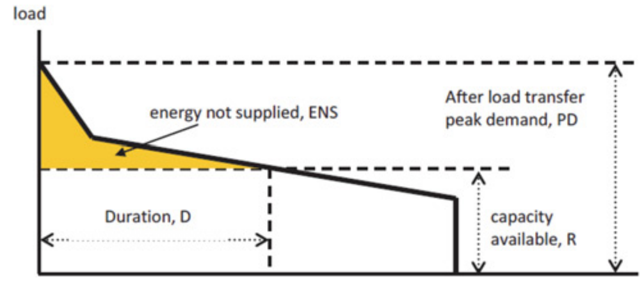

Fig. 2 *Example of how the LDC is used to calculate the ENS when the network capacity is less than the peak demand*

(6) The EENS for that fault is then calculated as follows:
(a) *Customer supplies restored via urgent repairs.* The ENS is the product of the mean load point demand and the urgent repair time.
(b) *Customer supplies fully restored via switching.* The ENS is the product of the mean load point demand and the switching time.
(c) *Customer supplies partially restored by switching.* The customer load not supplied during the outage is modelled using the LDC. If the network capacity is less than the peak aggregate load point demand, the ENS will be equal to the area below the LDC but above the network capacity, as shown in Fig. 2; if the network capacity is greater than the maximum demand, the ENS will be zero.
(7) The EENS for that outage, s, can then be calculated as:

$$\text{EENS}_\text{s} = \sum_{c=1}^{C} U_\text{s} \cdot \text{ENS}_{\text{s},c} \tag{2}$$

where U_s is the annual unavailability, c represents a circuit section to which affected customers are connected, and C represents the set of circuit sections to which customers are connected.
(8) Steps 2–7 are then repeated to account for all the other sections on each 11 kV feeder; the sum of these is to establish the EENS of the network.

2.3 Risk arising from an overlapping outage

Overlapping (or second circuit) outages follow the same process as in Section 2.2, with the following differences:

(i) The p_0 term for single outages is replaced by the p_i term, which represents the probability of the prior circuit being unavailable – this will be close to 0, which means that the U_o values will be much smaller than the U_s values in the previous section (where p_s was close to 1). The p_i term is calculated separately for periods when there is ENS assuming urgent repair time and for other periods assuming non-urgent repair time for the prior section.
(ii) There are many more overlapping outage states than single outage states, in the case of the case study network there are 264 single outage states and 20,886 overlapping outage states. However, the contribution of the overlapping outages to the EENS is small, due to the low probability of occurrence. Consequently, outages beyond $N-2$ are not considered.

3 Case study and sensitivity analysis

This section includes a description of the motivation behind conducting sensitivity analysis, the parameters used in the sensitivity analysis, and the case study network.

3.1 Motivation

The accurate evaluation of the capacity value of an asset requires a complex modelling methodology to be applied. Mandating such a methodology for each asset would not be viable in terms of computational administrative burden [3], and therefore a data-driven parametric model is a preferable approach. Sensitivity analyses can inform the development of such a model by

Table 1 Mean, minimum, and maximum values for each reliability level parameter subject to sensitivity analysis

Reliability level	Max	Mean	Min
overhead lines (OHLs) (11 kV)			
failure rate (f/y/km)	0.012	0.054	0.186
remote control switching time (min)	10	15	25
manual switching time (h)	0.5	1	3
urgent repair time (h)	7	9	11
non-urgent repair time (h)	95	151	447
underground cables (UGCs) (11 kV)			
failure rate (f/y/km)	0.002	0.047	0.365
remote control switching time (min)	10	15	25
manual switching time (h)	1.5	2.5	5
urgent repair time (h)	6	12	24
non-urgent repair time (h)	224	328	494
primary transformers (<25 MVA)			
failure rate (f/y)	0.01	0.022	0.07
urgent repair time (h)	15	87	206
non-urgent repair time (h)	200	543	720
primary transformers (>25 MVA)			
failure rate (f/y)	0.01	0.018	0.06
urgent repair time (h)	15	97	206
non-urgent repair time (h)	200	543	720

examining the impact of changes in key parameters and uncertainty ranges obtained through a data-gathering exercise. These analyses serve two main purposes:

- Improve understanding of which parameters have the greatest impact on the security of supply evaluated using the EENS metric, and which parameters could be excluded from a pragmatic model.
- An understanding of how the data uncertainties affect the assessment of the security of supply, both in the present-day networks and in projected future network load scenarios.

3.2 Sensitivity analysis input data

The sensitivity analysis was carried out using the data shown in Table 1, which was based on published literature, National fault and interruption reporting scheme (NaFIRS) data, and expert elicitation from NPg [4–9].

3.3 Case study network

The case study network used for this paper is shown in Fig. 3. It is a real 11 kV urban network, primarily comprising underground cables (total length: 42.89 km), seven feeders and 56 load points, which supply 11,740 customers.

4 Results

The baseline risk analysis was evaluated in terms of EENS but was converted to customer minutes lost (CML) for ease of comparison with historical data from NPg. The average case gave an annual CML of 129,845. This result is in line with observed values taken from NPg fault reporting data, which gave CML values for this network of 207,475 and 106,876 for 2016 and 2017, respectively.

As described above, the purpose of the sensitivity analyses is to investigate how the risk to customer supplies is affected by relevant network parameters in order to establish the key network parameters determining network risk. The risk evaluation methodology described in Section 2 and the input data presented in Table 1 were applied to the case study network shown in Fig. 3. Fig. 4 illustrates the EENS levels for the three considered reliability levels (max, avg, and min). Voltage is kept fixed at 1.0 pu because it does not significantly impact the reliability indices.

From the sensitivity analysis results presented in this section we can make the following observations:

(i) The overall system reliability indices change approximately an order of magnitude from max to avg, and from avg to min reliability levels (see Fig. 4),

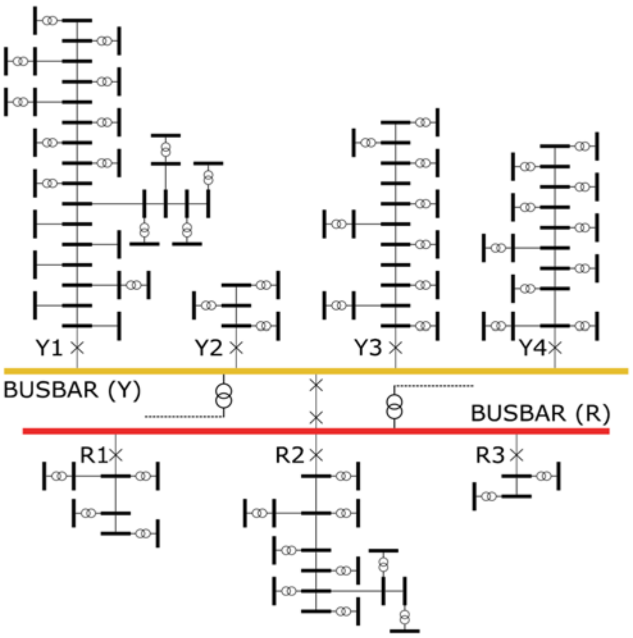

Fig. 3 *Case study network diagram. Open points between feeders and corresponding feeders supplied from adjacent primary substations are not shown*

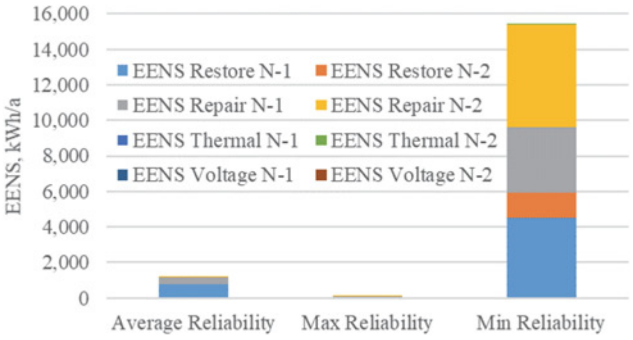

Fig. 4 *EENS for the case study network for different scenarios: max, avg, and min reliability levels; voltage is fixed to 1 pu*

(ii) $N-2$ events have zero EENS contribution at max reliability level; minor contribution (~4.5%) at avg reliability level; and account for about half (~46%) of the values at min reliability level.

5 Conclusion

This paper has presented a comprehensive method for evaluating the reliability indices for an 11 kV distribution network. The method has been used to evaluate the reliability of a real NPg distribution network, which is the initial case study for developing a pragmatic method for assessing the contribution of smart solutions to the security of supply. Sensitivity analyses have also been carried out to investigate how the performance of the network changes when key parameters are varied. Of the parameters investigated, the impact of the repair times and failure rates were found to be most significant.

The next stage of the project will be to apply network interventions designed to improve the security of supply. The demand will then be gradually increased until the system returns to the original level of reliability; the additional load accommodated is the equivalent load-carrying capacity (ELCC) of the network intervention. These ELCC values will then be used to produce empirical models or look-up tables that can be used to evaluate those smart solutions without having to employ comprehensive risk analyses of the type described in this paper.

6 Acknowledgements

This work was funded by Northern Powergrid via the NIA Project ‘Pragmatic Security Assessment’ (NIA_NPG_029).

7 References

1 ‘Engineering recommendation P2/7: security of suppy’ (Energy Networks Association, UK, 2019)
2 Imperial College London: ‘Review of distribution network security standards’, 2015
3 Konstantelos, I., Strbac, G.: ‘Capacity value of energy storage in distribution networks’, *J. Energy Storage*, 2018, **18**, pp. 389–401, doi: 10.1016/j.est.2018.06.002
4 Allan, R.N., Billinton, R., Sjarief, I., *et al.*: ‘A reliability test system for educational purposes – basic distribution system data and results’, *IEEE Trans. Power Syst.*, 1991, **6**, (2), pp. 813–820, doi: 10.1109/59.76730
5 Brown, R.E.: ‘Electric power distribution reliability’ (Marcel Dekker, New York, 2002)
6 ENA: ‘National fault and interruption reporting scheme (NaFIRS), national system and equipment performance 2009/2010’, 2010
7 ENA: ‘National fault and interruption reporting scheme (NaFIRS), national system and equipment performance 2012/2013’, 2013
8 ENA: ‘National fault and interruption reporting scheme (NaFIRS), national system and equipment performance 2017/2018’, 2018
9 ‘Information from Northern Powergrid DNO, UK’, 2020