

ENGINEERING RECOMMENDATION P2 REVIEW (PHASE 1)

# Findings of the qualitative review associated with the future development of the P2/6 distribution network planning security standard.

Energy Networks Association

**Report No.:** 16011094/200, Rev. 003

**Document No.:** 16011094/200

**Date:** 12/01/2016



---

---

---

Project name: Engineering Recommendation P2 Review (Phase 1) DNV GL Energy Advisory PSP UK

Report title: Findings of the qualitative review associated with the future development of the P2/6 distribution network planning security standard. Palace House 3 Cathedral Street London

Customer: Energy Networks Association SE1 9DE  
6th Floor, Dean Bradley House Tel: +44 (0) 203 170 8165  
52 Horseferry Road 04478894  
London  
SW1P 2AF

Contact person: D Spillet

Date of issue: 12/01/2016

Project No.: 16011094

Organisation unit: EA UK

Report No.: 16011094/200, Rev. 003

Document No.: 16011094/200

Applicable contract(s) governing the provision of this Report:

---

**Objective:**

This report presents the findings from qualitative analysis of the questionnaires sent to key industry stakeholders and interested parties regarding the present Engineering Recommendation P2/6 distribution network planning security standard and the future development of this standard. This qualitative analysis is carried out under sub work stream 2.0 of the P2/6 review process. Sub work stream 2.0 is one of a number of work streams being carried out to provide input into the suitability of a number of potential high level options for the development of the present P2/6 standard<sup>1</sup>. The options for development will be reviewed under work stream 2.9 and will be developed further with the DCRP P2 WG during work stream 3, prior to engagement through workshops with the wider stakeholder community in workstream 5 and subsequent options development, before going out to a formal consultation in workstream 6.

---

Prepared by:	Verified by:	Approved by:
--------------	--------------	--------------

---

Alan Birch  
Principal Consultant

---

Richard Druce  
NERA

---

Colin MacKenzie  
Head of Section

---

---

Copyright © DNV GL 2014. All rights reserved. This publication or parts thereof may not be copied, reproduced or transmitted in any form, or by any means, whether digitally or otherwise without the prior written consent of DNV GL. DNV GL and the Horizon Graphic are trademarks of DNV GL AS. The content of this publication shall be kept confidential by the customer, unless otherwise agreed in writing. Reference to part of this publication which may lead to misinterpretation is prohibited.

---

DNV GL Distribution:	Keywords:
<input checked="" type="checkbox"/> Unrestricted distribution (internal and external)	execution
<input type="checkbox"/> Unrestricted distribution within DNV GL	
<input type="checkbox"/> Limited distribution within DNV GL after 3 years	
<input type="checkbox"/> No distribution (confidential)	
<input type="checkbox"/> Secret	

---

---

<sup>1</sup> The full P2 review process is set out in the Project Initiation Paper "Engineering Recommendation P2 Review (Phase 1), Project Initiation Paper", DNV GL, 14/4/2015, circulated to all key industry stakeholders on 21/2014 and via an industry stakeholder engagement event in London on 1 May 2015.



Rev. No.	Date	Reason for Issue	Prepared by	Verified by	Approved by
001	20/9/2015	Draft for internal DCRP P2 WG review	A Birch	R Druce	C MacKenzie
002	13/11/2015	Draft for issue to DCRP P2 WG	A Birch	R Druce	C MacKenzie
003	12/01/2016	Final Issue	A Birch	R Druce	C MacKenzie



## Table of contents

1	INTRODUCTION.....	3
2	PHASE 1 P2 REVIEW .....	5
2.1	Background to the Project	5
2.2	WS 2 Option Evaluation Process (Phase 1)	6
2.3	WS2.0 Stakeholder Input	7
2.4	Options for the future development of the distribution network security standard	8
3	REVIEW OF QUESTIONNAIRE AND INTERVIEW RESPONSES. ....	10
3.1	Section 1 - Developing a better understanding of P2/6 strengths and weaknesses	10
3.2	Section 2 -alternative approaches To Security Standards and Regulatory and commercial considerations	17
3.3	SECTION 3: Real time Network Operation and security of supply	28
3.4	SECTION 4: Additional Questions and points for consideration	28
4	STAKEHOLDER VIEWS ON THE FUTURE SECURITY STANDARD - HIGH LEVEL OPTIONS. .....	30
5	SUMMARY OF STAKEHOLDER VIEWS.....	38



## Executive Summary

This document reports and summarises the results of the qualitative analysis undertaken by the Consortium (comprising DNV GL, NERA Economic Consulting and Imperial College) in the review of Engineering Recommendation P2/6. The objective of this qualitative study was to support the other mainly quantitative work streams of this project in reviewing key aspects of the existing P2/6 security standard and to highlight potential areas for development of a future UK distribution network security standard to P2/6.

The qualitative analysis is based on the review and analysis of our industry questionnaire containing a set of high level and more detailed questions to seek and gain the input of the many industry stakeholders regarding their opinions and views on the status, usability and adequacy of the existing P2/6 security standard and how this could be improved. To ensure that a wide range of inputs and views were captured and opinions recorded, all relevant industry parties and organisations were invited to provide their views and positions through a written response to the questionnaire. This has enabled the Consortium to build a fully representative understanding from industry stakeholders of their own views and opinions of the strengths and weaknesses of the existing P2/6 security standard and identify potential alternative approaches to security standards and regulatory and commercial considerations. Follow-up interviews were also held with key users of the existing P2/6 standard to clarify statements and opinions and to provide additional details to their organisation's responses.

The stakeholder responses have been analysed and reviewed to identify key themes that will be used as a basis for input to the development of a draft options report that will consider the benefits and problems associated with a set of high level options for the successor to P2/6. The draft options report will be developed with the DCRP P2 WG into a final options report ready for distribution to the wider industry for further formal consultation, leading to a final agreement and set of statements as to the future development path for a potential update to the existing security standard regime.

The stakeholder engagement outlined in this report is the first opportunity for industry stakeholders to input directly to the development of the options review process to identify a successor to the existing P2/6 security standard.

From the analysis of the various stakeholder questionnaire responses and details of the clarifications gathered by stakeholder interviews, a number of key themes emerged relating to the potential reform of P2/6.

The key themes identified and summarised from this review of the stakeholder responses included:

- Embrace the strengths of the existing standard
- Provide consistency with the regulatory framework
- Remain sufficiently intuitive and easy to audit
- New network technologies must be fully represented
- Provide a clear and consistent set of definitions
- Reflect network user expectations
- Introduction of Cost Benefit Analysis
- Treatment of network losses should not be included

- 
- Statements of requirements should remain prescriptive
  - Include the management of construction outages
  - Treatment of Extreme events

It should be noted that the views summarised in this report are those of the industry respondents. Statements made by respondents should not be taken to represent the views of the Consortium or the DPCR P2/6 Working Group. The analysis in this report is based on the questionnaire and interview responses, it does not argue or analyse whether the stakeholder views are justified or correct. Subsequent work in further work streams that utilise the summaries in this report will consider whether the stakeholder views are accurate and relevant for the inclusion in future development of a potential replacement security standard.

# 1 INTRODUCTION

In January 2014 the Distribution Code Review Panel<sup>2</sup> P2 Working Group (DCRP P2 WG) through the Energy Network Association<sup>3</sup> (ENA) engaged a consortium consisting of DNV GL<sup>4</sup>, Imperial College London (ICL)<sup>5</sup> and NERA<sup>6</sup> (the Consortium) in a project to carry out a full back to basics review of Engineering Recommendation P2/6. This engagement with the Consortium covers Phase 1 of a two phase project that would ultimately result in a new fully codified standard.

Phase 1 is essentially a comprehensive research, analysis and modelling engagement and consultation process to be carried out by the Consortium with direction and support provided by the DCRP P2 WG and the ENA. The objective of Phase 1 is to identify and agree a range of options for a future UK security standard and agree the most appropriate approach that should be taken into Phase 2 which is the codification of the new standard.

The project commenced in February 2015 with the development of a Project Initiation Paper (PIP)<sup>7</sup>. The PIP highlighted the key objectives of Phase 1 of the Engineering Recommendation P2/6 Review project to industry stakeholders and the process adopted to achieve these objectives.

The process to deliver the Phase 1 objectives outlined in the PIP consists of a number of work streams which can be broadly summarised as follows:

- **Work Stream 1;** set out the Phase 1 objectives and process, and included an initial engagement with all key industry stakeholders.
- **Work Stream 2;** identify, research and evaluate options for a future UK security standard.
- **Work Stream 3;** working with the DCRP P2 WG examine the deliverables from WS 2 and derive a range of options that will inform the processes in WS 5
- **Work Stream 5;** includes an industry wide workshop that will focus on introducing and discussing the deliverables from WS 3 (both quantitative and qualitative exercises). The workshop will critically examine the proposed options, their underlying assumptions and the implications on both the technical and economic models.
- **Work Stream 6;** further to WS 5, through a formal industry wide consultation gather written feedback on some of the more pertinent issues and concerns associated with the proposed new standard options.
- **Work Stream 7;** develop a tabulated view of all WS 6 consultation question responses and actions to be taken with regards to the final Phase 1 Report.

---

2 The Distribution Code Review Panel (DCRP) is the body responsible for overseeing the maintenance and development of the Distribution Code and its subordinate documents. Those subordinate documents include Engineering Recommendation P2/6. The ENA is the service provider to the DCRP for the physical maintenance of the Code and its subordinate documents.

3 Energy Networks Association is the industry body for UK energy transmission and distribution licence holders and is the voice and agent of the energy networks sector. ENA acts as a strategic focus and channel of communication for the industry and aims to promote the interests, growth, good standing and competitiveness of the industry. They also provide a forum for discussion among company members, and so facilitate communication and sharing of experience across the energy networks sector

4 DNV GL is a Global certification and advisory business working in the maritime, oil and gas, business assurance and energy sectors.

5 Imperial College London is a university of world-class education and research in science, engineering and medicine, with particular regard to their application in industry, commerce and healthcare.

6 NERA Economic Consulting is a global firm of experts dedicated to applying economic, finance, and quantitative principles to complex business and legal challenges.

7 DNV GL, NERA and Imperial College document "Engineering Recommendation P2 Review (Phase 1), Project Initiation Paper", report number 16011094/110, rev 001, 13/04/2015.

- 
- **Work Stream 8;** production of the final Phase 1 report that will lay out the arguments and all the supporting evidence for the development route for any new standard while critically highlighting the benefits of such a route.
  - **Work Stream 9;** will scope the work needed to implement the final recommendations from Phase 1 that will be undertaken in Phase 2 including a work programme for Phase 2 with an associated project plan.

This document reports on sub work stream 2.0 under work stream 2 covering a qualitative review of key aspects of the present P2/6 standard and potential areas for development of a future UK security standard to succeed Engineering Recommendation P2/6. The outputs produced through sub work-stream 2.0 will feed into the initial Options Report that constitutes sub work-stream 2.9.

Following this introduction section 2 provides the background to sub work stream 2.0. The review of the questionnaire and interview responses are summarised in section 3 with the impact on the high level options of a future security standard provided in section 4. A summary of the main stakeholder views and statements is provided in section 5.

## 2 PHASE 1 P2 REVIEW

### 2.1 Background to the Project

Engineering Recommendation P2 has been in place since the 1950s and has played a major role in the development of secure, reliable distribution networks. Whilst a number of changes have been made over the years, notably the introduction of P2/5 in 1978, the document has served the industry well for over 30 years.

P2 is a 'deterministic' standard and is largely focused around ensuring sufficient capacity is available to meet the 'peak demand' within a manner and timeframe consistent with the 'group demand' (or put simply, the size of network) in question. P2 is also 'risk based' to such an extent that larger 'load groups' are in general deserving of a higher level of security.

The most fundamental issue regarding the future evolution of the P2 standard is whether it prescribes economically efficient investments, given many changes affecting the energy market at present, including the (anticipated) prolific deployment of non-network technologies and the changing role of the customer. This gives rise to the need for a fundamental review of the baseline philosophy of distribution network operation and design to ensure that the UK Government's energy policy objectives can continue to be met in a cost effective and pragmatic way.

The requirement for a fundamental review of Engineering Recommendation P2 has been recognised by Network Licensees (i.e. the electricity Distribution Network Operators (DNO) companies and National Grid) for some time. The Licensees therefore believe that it is timely to undertake a comprehensive review of Engineering Recommendation P2 in relation to customer and system requirements and to develop an understanding of what is required to facilitate the long term development of networks.

The fundamental review of ER P2/6 is being directed by the Distribution Code Review Panel P2 Working Group (DCRP P2 WG) through the Energy Network Association (ENA).

The review is formed of two distinct phases. **Phase 1** is essentially a comprehensive research, analysis and modelling engagement and consultation process carried out by the Consortium with direction and support provided by the DCRP P2 WG and the ENA. Network licensees have no preconceived approach to future security standards. The spectrum of possibilities ranges from a modification and update of the current arrangements, development of a completely new approach starting from first principles, through to recommending removal of any deterministic planning standard, relying instead on DNOs' regulatory incentives and other legislation to motivate efficient network design. The essential task of Phase 1 is to identify, research, develop and communicate a range of options for the overall approach to structuring and detailing the appropriate level of network security standards and then to propose how such options can be evaluated. The Consortium will then evaluate these agreed options, and recommend the most appropriate approach that should be taken forwards into **Phase 2**, and ultimately codified.

Phase 1, poses some fundamental questions about the means of providing the most appropriate level of security of supply to customers, via a combination of network assets, customer owned assets, and both technical and commercial operational management techniques, and as such will be of great interest to many stakeholders. Hence as part of this phase it will be important to widely consult with such stakeholders throughout the process.

## 2.2 WS 2 Option Evaluation Process (Phase 1)

The aim of Work Stream 2 is to provide the analysis required to (1) understand the impact of P2/6 in its current form, and (2) identify the options for improvement and reform. The outputs produced through Work-stream 2 will feed into the initial Options Report that constitutes sub work-stream 2.9 and through a review process with the DCRP P2 WG finalise the options report in Work-stream 3 ready for wider industry engagement.

The analysis performed under Work-stream 2 is through a number of sub work streams covering a range of topics, and entails comprehensive desktop research, modelling of key issues and gathering of stakeholder input activity to identify the current impact of P2/6 and possible impacts from alternative security standard options. Amongst the primary areas of focus are the following:

- **Work Stream 2.0** Engagement with industry regarding questions around the existing P2/6 distribution security standard and possible future options, including a qualitative analysis of responses regarding their possible impact on any future alternative standard option.
- **Work Streams 2.1** Provision of a scope and framework for assessing security performance and measures of characteristic network designs;
- **Work Stream 2.2.** Analysis of the distribution network service quality performance associated with the present network design standard and alternative options for its update;
- **Work Streams 2.3.** Assessment of risk associated with asset replacement, common mode failures and high impact events;
- **Work Streams 2.4.** Analysis of the impacts of Smart Grid solutions on security of supply;
- **Work Streams 2.5.** Assessment of impacts of alternative control and operation strategies on security of supply;
- **Work Streams 2.6.** Loss inclusive design of distribution networks and impact on security of supply;
- **Work Streams 2.7.** Interface between distribution network standards and the regulatory framework (RIIO), EU codes, capacity mechanism and balancing services significant code review, and defining the interface between distribution network standards and IIS and SQSS.
- **Work Stream 2.9** Development of the initial options for a future distribution security standard based on evidence from the quantitative analysis in Work-streams 2.1 to 2.7, and the qualitative analysis from Work-stream 2.0.

Work Stream 2.0 relates to the gathering of input from stakeholders that support some of the above sub work stream elements and also provides a qualitative analysis relating to the existing P2/6 standard and proposed alternative options. WS2.1 to WS2.6 predominantly relate to the techno-economic model and quantitative analysis performed. The results of the quantitative and qualitative analysis from the various sub work streams are used in the initial options report developed under sub work stream 2.9.

The focus of this report is the industry engagement and response to questions concerning the existing P2/6 standard and possible future standard options and the qualitative assessment of the impact of the industry response. Subsequent sections describe the approach in detail associated with work stream 2.0.

## 2.3 WS2.0 Stakeholder Input

A key part of the P2/6 Phase 1 review is to gain a detailed understanding of the position of the many stakeholders as a starting point for our qualitative analysis. The most effective way to understand the current status and thoughts of the industry is through feedback directly from the stakeholders.

The qualitative analysis tasks began with a set of high level and then detailed questions to seek and gain the views of the many stakeholders regarding their thoughts and views on the status, usability and adequacy of the existing P2/6 security standard and on the future development of the standard. To ensure that the views and comments for all relevant industry parties were sought and recorded, the stakeholders were split into two broad categories:

1. **Category 1** - stakeholders that make use of ER P2/6 on a regular basis and where P2/6 has a direct impact on their business (DNOs and NGET) and those who have responsibility for oversight (DECC and Ofgem). The questionnaire was aimed at those in the DNOs that have direct responsibility for setting planning policy, operational engineers (i.e. those that have experience of operating the network or managing outages), LCNF teams (i.e. those looking at future developments and new technologies) and regulatory/commercial teams (i.e. those concerned with the impact of any change to P2 in terms of change control and financial management). Each one of the stakeholders was provided with a copy of the questionnaire to complete covering a range of pertinent areas. Having reviewed each questionnaire submission the Consortium held interviews with key representatives for the DNOs, NGET, DECC and Ofgem to ensure our understanding of the questionnaire responses and seek views and feedback on any additional topics that were not explicitly included in the set of detailed questions..
2. **Category 2** - the wider group of interested parties and industry participants who do or may have an interest in the P2 review process to ensure that relevant industry participants have had a chance to provide significant input into the final analysis. This wider group of stakeholders include representatives from Offshore Transmission Owners, independent DNOs (IDNOs), and trade bodies and organisations covering traditional and renewable resources: solar, conventional and renewable generation, hydro generation, demand side response and domestic customers. Each stakeholder in this wider group was sent the same questionnaire provided to the DNOs, NGET, DECC and Ofgem to ensure full transparency. However, since the original full questionnaire included some specific questions directly designed to elicit responses from the DNOs (as the main users of ER P2/6 to help in the quantitative analysis) which may not have been relevant (or too detailed) for the wider set of industry participants, guidance was provided on which questions may be pertinent. That said the wider group of stakeholders were offered the opportunity to answer any of the questions posed in the questionnaire to ensure all points of view were captured. The consortium reviewed all questionnaire responses and where necessary conducted follow-up calls or correspondence to clarify responses.

The questionnaires and interviews were designed to support the review analysis activities, particularly the qualitative analysis, and to ensure that relevant industry participants have had the opportunity to provide significant input into the final output.

The purpose of this questionnaire was to document the experience and comment gathered from different sources so that relevant information, current practices and future views could be identified and utilised during the P2 review process.

The questionnaire is presented in Appendix A for information and consisted of four main areas designed to help gather stakeholder views and elicit feedback on:

- 
1. Developing a better understanding of the strengths and weaknesses of ER P2/6;
  2. Alternative approaches to Security Standards and Regulatory and Commercial considerations;
  3. Real time network operation and security of supply, and
  4. Additional questions and points for consideration.

This last area was included to allow all respondents to raise their own questions and respond to these where they felt these were important.

The list of organisations and companies invited to respond to the questionnaire is provided in Appendix B. In total the Consortium received completed questionnaires from 14 respondents plus two organisations that provided verbal responses through interview only. A number of respondents represented trade bodies and organisations and hence represented the views of many member organisations. The Consortium and the DCRP P2 WG believe that all key stakeholders have been invited to respond to the questionnaire and that the views of the majority of key interested stakeholders have been received.

All questionnaire responses were reviewed and analysed to develop the qualitative analysis presented in this report and support some of the quantitative modelling and analytical work streams that are part of the P2 review process. This work is in support of the DCRP P2 WG's aim to determine the future development route of the P2 security standard. The comprehensive range of high level options for the future development of the P2 security standard are summarised in section 2.4.

The key findings from the questionnaire responses and any follow up interviews have been further analysed to determine how the responses could impact the qualitative analysis of each of the high level options for a new standard. The main points and outcomes of this analysis are summarised in Section 4.

## **2.4 Options for the future development of the distribution network security standard**

The Phase 1 review of the future distribution network security standard considers a comprehensive range of high level options including:

1. Retain the existing P2/6 standard as is.
2. Enhance P2/6 but retain the deterministic nature/structure. Enhancements considered included:
  - a. Non-network solutions – generation, storage, DSR, advanced automation.
  - b. High impact low probability events.
  - c. Long term outages for asset replacement
  - d. Common mode failures.
3. Replacement of P2/6 with obligations to perform probabilistic CBAs
4. A hybrid standard with a deterministic structure and obligations to perform probabilistic CBAs
5. Complete removal of the P2/6 security standard.



The Consortium is evaluating the range of options using the cost benefit framework established by Imperial College under sub work stream 2.1<sup>8</sup>. This cost benefit framework considers the quantitative costs and benefits of:

- Different service quality standards delivered to end customers, assessing frequency and duration of outages together with risk profile and robustness associated with construction outages, common mode failures and high impact events.
- Options for incorporation of demand side response, distributed generation and energy storage technologies in the future network design standards is considered, while considering application of advanced automatic control schemes and/or area-wide operational measures that might contribute to security.

Furthermore, Imperial College has also considered the appropriateness of conducting additional research within present LCNF projects in order to inform their analysis and the development of alternative distribution network standards.

The overall evaluation framework also needs to account for more qualitative considerations, such as the transparency and simplicity of proposed design standards, and the ease with which DNOs' compliance with these standards can be appraised in the future – for example to demonstrate licence compliance. The stakeholder engagement process was designed to assist in accounting for these more qualitative aspects in the overall evaluation.

---

<sup>8</sup> Engineering Recommendation P2 Review (Phase 1), Project Initiation Paper, ENA, Report No. 16011094, rev 001, 13/4/2015. Section 3.1 outlines details of the Framework for the development of future network design standards.

### 3 REVIEW OF QUESTIONNAIRE AND INTERVIEW RESPONSES.

This section sets out the questions structured to obtain stakeholder views and feedback in the four key areas, the last being an opportunity to feedback on any questions not raised in the questionnaire that may however be of particular importance to a stakeholder:

1. Section 1 - Developing a better understanding of P2/6 strengths and weaknesses.
2. Section 2 - Alternative approaches to security standards and regulatory and commercial considerations.
3. Section 3 - Real time Network Operation and security of supply.
4. Section 4 - Additional Questions and points for consideration.

All stakeholder responses were treated as confidential and so no respondents are identified with any response. The responses to each question have been reviewed and where there is a clear view provided by groups of stakeholders the view, stakeholder numbers and stakeholder business interests is indicated. Also where single stakeholders raise an important point or issue these are also presented. It should be noted that section 3 of the questionnaire was designed to elicit feedback and thoughts regarding the real time operation of distribution networks. This section was included in the questionnaire to gain views on different aspects of the application of IT and real time operation. The questions were not directly related to the stakeholder views on aspects of the existing or any future security standard but used to supplement and expand some of the detailed analysis of alternative control and operation strategies on security of supply. For this reason, the questions have been included in this report, (for transparency) but none of the responses from any party have been included as they were not relevant to the subject matter of this review.

Please note that all statements and opinions expressed in section 3 are those of the respondents. Statements made by respondents should not be taken to represent the views of the consortium or working group.

#### 3.1 Section 1 - Developing a better understanding of P2/6 strengths and weaknesses

In the following questions stakeholders were asked views and feedback to aid a clearer understanding of the (perceived) strengths and weaknesses of the existing security standard. All responses have been reviewed and summarised to provide the following points of view and supporting rationale.

##### Question 1.1:

Is the present network design standard efficient?

Does it deliver value for money to all network customers?

In other words, does it balance the cost of network infrastructure with the security benefits delivered to distribution network customers?

##### Category 1<sup>9</sup> stakeholder responses

Respondents agreed that all Network Owners and operators are obliged to plan and operate their networks in an efficient, economic and coordinated manner and this has been largely supported and guided by the existing P2 standard over the years. This approach has complemented licensees activities in a clear, robust and auditable manner which has not only supported a broadly consistent planning basis

<sup>9</sup> See section 2.3 for the definition of category 1 and 2 stakeholders.

across organisational boundaries but provided a basis by which customer requirements may be easily articulated, and their supporting need for consent and investment demonstrated.

In general some respondents indicated that in their view, it was difficult to determine if the design standard was efficient or not, but others expressed a view that P2/6 does balance the cost of loss of supply against network assets. Views were also expressed that the costs and values in the standard are based on 1970s figures, both of which will have changed substantially, so it is clear that the value of lost load in P2/6 will probably be understated, whilst the costs are probably too expensive in real terms. Respondents indicated that P2/6 tries to balance costs and benefits, its shortfall is that it only looks at the costs of circuits, and there is general consensus from respondents that it is out of date.

Respondents were clear that P2 in its various versions has stood the test of time and facilitated the construction of networks that deliver the current network performance experienced by customers and the associated level of underlying risk. The level of network security for demand connections currently seems to balance the costs and benefits – it is generally reasonably received by demand connections with the level of security generally meeting their expectations. Further, some respondents expressed the view that as all GB DNOs have developed networks in accordance with the same guidelines it is now difficult to form a view of whether the GB system performance / cost are efficient or inefficient.

Some DNOs took the view that the current standard was efficient as it considered the minimum plant for a specific level of security however, this minimum level is based upon maintenance outages whereas, given the age of the network, we are now heading into a period of asset replacement where construction/replacement outages will be more common place.

Respondents also indicated that that P2/6 does deliver value for money on the basis that the minimum standard is simple and easy to implement. Where customers require higher levels of security, they have the option to pay for additional infrastructure. However, the exclusion of innovative solutions means that value for money could be further improved upon.

Respondents also noted that the existing P2/6 works well for networks designed to accommodate conventional demand which tends to naturally be geographically centred around existing infrastructure and has predictable load distribution and load densities. It was the view of the majority of respondents that for Generation customers however there is a clear disjoint between their expectations regarding the level of security and what P2/6 delivers. However there also remains a high level of resistance against any greater level of funding of the enhanced security they believe they should receive.

### Category 2<sup>10</sup> stakeholder responses

Some respondents expressed the view that the current network design standard was efficient for demand customers but there is a major exception in that it does not include distributed generation connections. It is believed that it does provide value for money and has the benefit that it is relatively simple to interpret and apply.

There was some feedback from respondents to indicate that as a network user, it was not possible to know whether the present network design standard was efficient.

<sup>10</sup> See section 2.3 for the definition of category 1 and 2 stakeholders.

Respondents agreed that the fundamental assumptions on which P2/6 has historically been based are changing and the current design methodology is not flexible enough and does not capture the future needs of the network and its users. Demand profiles are changing due to changes in energy efficiency and customer behaviours and these will change further as intermittent embedded generation, electric vehicles and local electricity storage evolve. It was further suggested by some respondents that the P2/6 document could be improved with some worked examples about how to use the various tables to perform a DG assessment. That would make the document more accessible to interested parties not directly affiliated with the DNOs.

One respondent indicated that P2/6 may be considered as an 'invisible' document to the wider industry and vast majority of customers (demand and generation) and that this situation should change to promote the security standard to a wider audience as any dilution to security arrangements (and subsequent restoration times) would not be considered to be acceptable by network users.

One respondent noted that the current standard provides clarity to both designers and customers with regard to standard of security and connection expectations. It was also noted that P2/6 does not and was never intended to 'balance the cost of network infrastructure' (i.e. reinforcement costs). It remains a tool to be used with other Planning Manuals in order to develop an efficient and co-ordinated distribution network in support of the DNO licence condition.

## Question 1.2:

What, in your view, are the strengths and weaknesses of P2/6?

How might it be improved?

What should be the key features of the new security standard (if required)?

### Category 1 stakeholder responses

In general the majority of responses indicated that P2/6 was originally well founded and had stood the test of time well during times where there was network expansion but the primary use and requirements remained more or less consistent. However now there was a requirement to make some much needed updates to accommodate the developing state of distribution networks and prepare for future changes and new asset types.

In general the following strengths were recognised by respondents:

- The ER in its current version has stood the test of time and underpins fairly good system performance.
- Implements probabilistic assessments in a deterministic manner.
- Increases the required network resilience with increase in demand / number of customers.
- Provides resilient networks that cater for a wide range of contingencies especially for large load groups.
- Simple for all stakeholders (ranging from government/regulators to customers) to understand and interpret.
- Sets out a long term clear minimum standard required for the networks to meet (or exceed if required).
- Provides a common framework for price control baseline.
- Well understood and aligned to current design practice, forms the basis of DNO planning methods.

- Assumes a top down flow of energy and places the greatest resilience at the top levels.

In general the following weaknesses were identified by respondents:

- Does not imply the necessary level of network performance at lower voltage levels (11kV and below), the IIS (Interruption Incentive Scheme) tends to require a greater level of security than that prescribed by P2/6 at lower voltages, but is only an incentive mechanism rather than a design standard.
- Does not include statements or treatment of DSM, generation, other network solutions (smart grids) or provide a degree of “future proofing” for new technologies.
- Does not consider the security of the connection between the generation point of connection and the network when assessing the security contribution from that generation.
- Does not make provision for real-time considerations which will become more prevalent as smarter technologies and more flexible, controllable and variable load are more widely adopted within GB distribution networks.
- The requirements and forecasting for demand groups <1MW should be better and more clearly defined and the derivation of “circuit capacity” may be inconsistent.
- Assumes all customers value electricity equally at all times and probably at a rate that understates modern expectations.
- Does not cater for the frequency of interruptions.
- Some outages are permitted for (unlimited) repair time.
- Does not consider circuit length, routing or locations.
- Lack of clarity on what maintenance period load should be.
- Lack of clarity on whether busbar faults should be treated.

Respondents identified a number of key features any new standard would need to include:

- Consistent with the existing regulatory framework.
- Be simple / easy to apply, with unambiguous statements and consider the availability and cost of planning staff required to apply a methodology.
- Sufficiently intuitive and easy to audit.
- Easy to explain in public enquiries and/or wayleave hearings.
- Facilitate efficient investment / demonstrates ESQC (Electricity Safety, Quality and Continuity Regulation) compliance.
- Align with, or accommodate other regulatory incentives (e.g. IIS).
- Reflect network user expectations / customer willingness to pay for levels of security.
- Meet customer requirements.
- The standard should not include losses as a design driver but should ensure stronger coordination with other design processes that consider losses.
- Needs to be prescriptive enough to ensure all DNOs are designing to the most economically efficient and common sets of methods to provide supply of security that offers the best value for customers but also balanced with adaptability to facilitate new/innovative methods of managing the network / network demand.
- Inclusion of a definition of Firm Capacity might help – although not including one was a specific decision taken by the team drafting P2/6.

### Category 2 stakeholder responses

Respondents generally agreed that the current standard provides definitive guidance to security of supply arrangements and these arrangements must be continued and remain the focal point of any

revised or updated standard.

Also, the key feature of any amended document must be to retain the clarity and transparency of the existing document, to retain the standards for demand type connections and to supplement the document with agreed standards for distributed generation connections.

Further, it was indicated that P2/6 and its predecessors have always sought to be rationally based, evaluating investment cost and risk on a probabilistic basis, rather than the more simple deterministic (and arguably less demonstrably economic) transmission standards. A future P2 would need to incorporate additional flexibility to cater for a more widely divergent customer base and also be able to respond more strategically – for example by investing ahead of need, when the longer term economics suggest that this is a less costly option.

Respondents also indicated that the present standard provides a robust set of design parameters for design engineers and the expectation of customers. Whilst changes can be made it would introduce risk and potentially remove a level of comfort for customers. This will need to be considered and highlighted to customers who wish to rely on alternative solutions to their supply.

The following P2/6 benefits and issues were generally recognised by respondents:

Strengths:

- Short and mainly clear guide lines.
- Clear and easy to understand and implement.
- Use of defined terms.

Weaknesses

- No treatment of DSR but some guidance is provided for DG so appears biased.
- Long term investment may not be adequately supported.
- Not clear how to use the assessment methods for DG (tabulations).

Improvements

- DSR **must** be introduced into the document and treated in a clear, fair and robust manner.
- Full and clear balanced representation of DG / DSR / storage and other network technologies.

### Question 1.3:

How does “whole life costing” impact on the planning/designing your network?  
Do you feel that “whole life costing” is adequately captured within P2/6?

While there is no single definitive definition of “whole life costing”, we would like to understand the cost components considered by each DNO. For the purposes of responding to this question, the working definition of “whole life costing” would be: “the systematic consideration of all relevant associated costs of network assets, including: construction, ownership and maintenance”.

We are also interested in costing definitions which may be provided in the response.

#### Category 1 stakeholder responses

Respondents provided mixed views as to the use and impact of “Whole Life Costing” but generally it was stated that whole life costing did impact in the design of the networks in some form.

One DNO indicated that "Whole life costing" was probably more applied to the assets and to design considerations that were not relevant to P2 until quite recently. Although DNOs' policies would often have some element of whole life costing in them, actual decisions could be more short term, driven by the current regulatory incentives; incentives which change at each price control. The introduction by Ofgem of CBA for many routine investment or management decisions has impacted DNOs' behaviour with more focus now towards long term whole life costing and NPV minimisation.

Other DNOs indicated that "Whole life costing" is a factor but perhaps not a key driver when designing network solutions and deciding on overall internal design standards, including which equipment was suitable for differing situations. However DNOs are also mindful of the obligation to offer the minimum total cost of connection to connecting customers and so although "whole life costs" affects the overall design standards and strategy the solution will always aim to minimise up-front costs.

Another DNO indicated that they did not believe that P2/6 required them to take whole life costing into account and that it was something that needed attention. Given that there is no single definition of whole life costing and given the move away from conventional solutions, they suggested that the definition is evolving, but it did not prevent a DNO from considering whole life cost as part of efficient network investment but doing so may be a departure from P2/6.

A further DNO supported this view, they stated that whole life costing was not a concept explicitly covered by P2/6 but was included in the general obligation to develop an economical, efficient and coordinated distribution system. They indicated that there was a need to consider the time scale for assessing 'whole life costs', is it the lifetime of the individual assets used on the network or the lifespan of the network itself?

#### Category 2 stakeholder responses

No responses from category 2 stakeholders were requested or received for this particular question, which was aimed specifically at category 1 stakeholders.

#### Question 1.4:

We are aware that DNOs treat construction outage management differently to fault conditions. How do you quantify the increased risks of customer interruptions associated with long term construction (or maintenance) outages?

#### Category 1 stakeholder responses

DNOs indicated that there is some assessment of risk of interruptions from asset failure during long term outages, (but one DNO indicated that there was risk quantification) as longer term outages carry a larger CI and CML risk whilst they cannot do anything about faults occurring. Both fault (un-planned) and planned outages are risk assessed against a next single circuit fault based on customer numbers and potential IIS costs. The IIS consequences of outages are treated as part of an outage assessment and will tend to drive additional risk mitigation measures. It was indicated that the financial consequence and importantly the financial risk was a sensitive area to discuss in more detail.

DNOs indicated that the overall risk assessment for construction outages is used to prioritise or resource the mitigation of faults during planned outages accordingly to minimise the risk to the customer and so

to minimise the potential financial impact and balance the reputational impact on them. It was generally stated that construction risks were often viewed as being more controllable by the DNOs as there is the opportunity to plan and evaluate mitigation measures. Part of the risk mitigation approach identified was to take construction outages during a period where the network is under less stress and more amenable to reconfiguration and switching. Such an approach ensures the remaining network is not placed at unnecessary risk but that the risk is still managed to be compliant with P2/6. Hence construction outages are almost always scheduled for periods of lower demands so that risks are minimised. However, while this has worked well in the past it may be more problematic in the future to determine such periods. It was noted that due to the expected change of customer behaviour, future changing demand patterns may mean that predicting a season when the network was less stressed may not be possible (or at least more difficult) leading to greater uncertainty when planning long term construction outages.

#### Category 2 stakeholder responses

Responses were not requested for this question, but one respondent noted that construction outages allow significant forward contingency planning and mitigation and generally may be arranged at times of lower network risk and lower network demand so the impact on consumers is generally less than under fault conditions. Load transfers and temporary generator support are also more viable for planned construction outages than for fault outages.

#### Question 1.5:

In your view, should the planning standard include an explicit requirement for DNOs to account for the loss inclusive network design?

Do you have any suggestions regarding the form that such a requirement should take?

#### Category 1 stakeholder responses

DNOs generally agreed that Security of Supply and Electrical Losses were two different components of what they need to manage, providing inputs into an overall system design policy and that Electrical Losses were a separate issue with their own drivers. Respondents indicated that the network resulting from a losses efficient design may provide an additional level of security in some cases, which might be modified by requirements of the security standard, but the underlying drivers were separate. DNOs believe the main focus of the security of supply standard should remain as it is, i.e. focus on the minimum design standard for different levels of demand. Delivering an economic and efficient network is an important element of the licence obligation so loss inclusive network design should not to be duplicated or reinstated as part of security supply planning standard. It was noted that since all DNOs have an obligation under LC49 to reduce losses their assessment could be factored into the economic analysis providing a trigger point to support further works.

One DNO indicated that there seems to be a contradiction in the regulatory drivers that needs to be addressed in that the minimisation of cost in order to meet the minimum security of supply standard results in higher network utilisations, which results in higher losses. This creates a tension between P2 compliance and losses reduction; clearly P2 must take the lead, but this may then force the DNO to adopt an approach to network design that is not necessarily supportive of a low loss network.

### Category 2 stakeholder responses

No responses from category 2 stakeholders were requested or received for this particular question, which was aimed specifically at category 1 stakeholders.

## 3.2 Section 2 -alternative approaches To Security Standards and Regulatory and commercial considerations

In the following questions stakeholders were asked for views and feedback regarding potential alternative approaches to the existing (and any future) security standard and the impact of Regulation and commercial propositions on the security standards. Once again, all responses have been reviewed and summarised to provide the following points of view and supporting rationale.

### Question 2.1:

If P2/6 were enhanced to account for non-network technologies (e.g. storage and DSR/DSM), what types of changes to the existing standard do you think could be implemented to achieve this, and what are the advantages and disadvantages of these alternatives?

### Category 1 stakeholder responses

All DNOs agreed that there was a need to understand the reliability and availability of non-network technologies to deliver security services, not all DSR provide the same level or have the capability to provide the same level of reliability, so methodologies to identify the extent of DSR effectiveness on network design would need to be identified. DNOs generally agreed that there would need to be a robust assessment of the contribution that contracted services could make to the network and the level of security that could be provided, but it should be left to the DNO to quantify these contributions perhaps through the use of reliability factors rather than prescribed by the standard. It was noted that where the DNO has direct control of the demand then this may have a clearer contribution to security but there were still many variables for security risk that must be taken into account.

One DNO noted that large volumes of smaller security measures such as domestic storage or customer self-sufficiency should statistically provide a greater reliability of support for network security through natural diversification. Also, they noted that non-network technologies could only be incorporated into security of supply if suitable commercial agreements were in place and that limits on how much could be relied on may need to be imposed.

Respondents also generally agreed that DSM and probably storage (depending on its operation) would introduce an element of market behaviour that is more complex than the market interactions associated with generation. These market factors need to be understood and incorporated in the security methodology. There is a level of market interaction and potentially conflicting commercial incentives that may cause problems to deliver the request for demand response.

One DNO indicated that the specific inclusion of DSR was unnecessary as the important issue was the reliability of supply delivered to customers, not how it is achieved. They indicated that putting any technology specific requirements into a standard is likely to inhibit some innovative approaches for future network development, but agreed that it might be useful to provide some technology specific guidance if the risks of doing this were properly assessed.

## Category 2 stakeholder responses

Respondents agreed that any revision to P2 must take into account new technologies, including (but not limited to) energy storage and DSR that are approaching roll out in the UK and they must be supported to provide their full value in the market and on the grid system operation. It was suggested that these customers would expect the same level of clarity and transparency as enjoyed by demand customers – if not the same level of restoration times, perhaps restoration times should be the subject of industry discussion and debate and at the earliest opportunity.

One respondent commented that in principle storage and DSR/DSM are controllable, however, unless the DNO is able to persuade customers to behave in a way that supports distribution network operation, their potential benefits may not be achievable. In a market based system this means that DNOs have to be able to procure certain services from customers but this must be completed in a fair and equitable manner across all customers.

## Question 2.2:

Technologies such as embedded generation, storage and DSR/DSM may behave in a way that is supportive to the distribution system (e.g. in response to time of use distribution tariffs), or they may behave in a way that is supportive to the power system as a whole (e.g. in response to power price signals). Should this issue be included in system planning and if so, how?

## Category 1 stakeholder responses

DNOs generally agreed that as a minimum or baseline the DNO needs to be able to understand how the technology was being deployed for each project / installation and the extent to which it could offer support to the DNOs system (including operational constraints and levels of reliability) but it was difficult to understand how such technology may be used for system planning purposes.

Respondents also indicated that it was clear that there needs to be interaction between the security standard, any form of licence obligation and the energy market. It was suggested that a cap on the level of non-network solutions could be defined to protect the network security from dependency risks such as market changes or market participation behaviour that are much shorter term than the planning time horizon.

Some concern was stated by DNOs regarding the use of Time of Use Tariffs and if they could be relied upon to reduce demand when required, how the DNO would actually implement the request for demand reduction and would customers provide the required response at the appropriate time period. It was stressed that these activities are commercial and need to be treated as such so should not be exploited or relied upon to the extent of more traditional technical solutions. There was concern over the ability to forecast the “true” demand and the issue of load recovery post event and while they may support local security, it is not clear the effects on diversity as the demand increases. It was noted that demand reduction measures implemented at LV would also contribute to higher voltage level demands and this needs to be accounted for within any new standard.

Respondents highlighted that the security standard should enforce the priority of DNO-led commercial arrangements, rather than TSO-led arrangements. Clustering of technologies may cause localised constraints on the distribution network and it should be possible for the DNO to manage these commercially if viable.

## Category 2 stakeholder responses

Respondents agreed that the revised security standard should maintain the current emphasis relating to security of supply but be further developed to include renewables and DSR/storage as they are key contributors to the successful grid of the future.

It was noted by respondents that in a market based system, technology behaviour will respond to market incentives that may be perverse and not support the local network requirements. For example with an energy based FIT or CfD, a renewable generator is not incentivised to operate in a way that supports a DNO, as there is no financial incentive to do so. If a DNO wishes to use embedded generation, storage or DSR/DSM to achieve security of supply then those technologies should be subject to contracts and controls which ensure that their support is delivered in a suitable manner when needed.

## Question 2.3:

Supposing that P2/6 were replaced by an obligation to perform stochastic cost-benefit analysis when planning the network:

- How prescriptive do you think such an obligation would need to be in terms of specifying the modelling approach and assumptions that should be used for such studies and the options that they should consider?
- What process of oversight/approval by Ofgem would you consider necessary/proportionate? For instance, scheme-by-scheme approval/audit, approval of DNO-specific or industry-wide modelling tools/modelling methodology statements?

## Category 1 stakeholder responses

It was generally felt by DNO respondents that the practicalities and additional costs of carrying out a stochastic assessment for each HV and EHV scheme was unrealistic; there would need to be a prescriptive approach for at least the most common scheme studies and there would be difficulty quantifying the benefits to customer groupings. In addition, it was felt that agreement would be required on the risk assessment process and parameters that would be essential to ensure consistent application, this would require inputs from Ofgem to develop and approve the methodology and there would be an issue over the oversight and governance that was prescriptive enough to ensure all DNOs were designing to the most economically efficient Supply Security to offer the best value for customers. This should be balanced with adaptability to facilitate new/innovative methods of managing the network / network demand.

It was also indicated that discretion should be left to the DNO to decide on the level of risk they are prepared to accept versus the economic impact. DNOs indicated that they would respond to the incentives placed on them by Ofgem to implement the solution they see fit.

DNO respondents advised that there seems to be varying methods in how group demand is identified. There should be standard guidance on how future demand might be estimated, e.g. how to use historic outturns, how to take account of variability due to weather or how to take account of diversity among sub-groups, but not rules on how future demand should be estimated.

There was concern expressed by DNOs regarding the time and resource impact on the DNO planning

departments and that Ofgem may become more involved with network designs, which is not practical or feasible given the level of resources available to all parties.

One DNO indicated that the adoption of CBA modelling by DNOs and Ofgem to inform decision making is generally a positive step and adopting a decision making framework would be appropriate and necessary, also the industry must avoid the black box solution and any prescribed requirement must be simple and transparent – a view supported in general by all DNOs.

#### Category 2 stakeholder responses

Responses were not requested for this question but one response was provided to suggest that the approach used by P2/6 is effective and easy to apply for the majority of staff employed in the design work. To create a more time consuming and costly method could prove to be expensive and add little value.

### Question 2.4:

How do you believe your/DNOs' asset planning policies would change if P2/6 were removed entirely? What are the pros and cons of removing P2/6 completely?

Absent P2/6, would the current suite of outputs obligations and financial incentive mechanisms implemented through RIIO-ED1, as well as any other applicable regulations that affect your asset planning, be sufficient to encourage efficient levels of investment to ensure security of supply?

#### Category 1 stakeholder responses

Some DNOs indicated that there would initially be no change as P2/6 was largely irrelevant for Group Demands below 100MW and that the IIS incentive drives system design, to ensure that losses of supply are minimised both in number and duration. Although it was agreed that this incentive could be altered/removed by Ofgem and it did not constitute or seek to replace a design standard.

DNOs indicated that there is a licence condition to "Plan and develop the distribution system in accordance with a standard not less than that set out in Engineering Recommendation P2/6", a requirement under the Electricity Act that was designed to ensure consistency across distribution networks and to a common standard. Such a standard would still perhaps be required to ensure some level of consistency, but it was suggested that any new standard should recognise the use of "Alternative" approaches in providing system security. It was noted that the additional CI/CML impacts, as a result of including such approaches as DSM & Embedded Generation, must be taken into account and not penalise the DNO in taking on the additional risk, but rather perhaps reward a DNO for actively taking on the risk.

One DNO argued that removing P2/6 entirely would change DNO investment behaviours and overall financial modelling/decisions, and that some DNOs may focus on CI/CML benefits and invest heavily and some may defer system reinforcement and manage interruptions while some DNOs may do a combination of both options.

#### Category 2 stakeholder responses

No responses from category 2 stakeholders were requested or received for this particular question, which was aimed specifically at category 1 stakeholders.

## Question 2.5:

We are exploring the hypothesis that planning standards are not required if network users can contract for the degree of security of supply they want. For instance, some consumers can already negotiate with the DNO regarding the “firmness” of their connection, making a trade-off between cost and the degree of security they purchase:

- Should the planning standard prescribe the amount of network capacity for smaller sizes of group demand (e.g. for class supply A-C<sup>11</sup>)?
- Should the planning standard prescribe the amount of network capacity provided for generators, given that they can negotiate with the DNO regarding the degree of “firmness” provided through their connection to the distribution system?
- How, if at all, does the need for a prescriptive planning standard change as consumers receive smart meters, and so could (in theory) receive signals through tariffs regarding the availability of network capacity in real time? For instance, real time DUoS charges could signal scarcity of network capacity when it arises, and encourage consumers to curtail load.

### Category 1 stakeholder responses

DNOs were generally not in favour of completely removing P2 and its obligations. There was agreement that for Class A-C, IIS is a stronger driver, but (again) it should be remembered that IIS is a regulatory incentive and so provides no basis for enforcement whereas compliance with P2 is both a Distribution Code and licence obligation. P2/6 is a “one size fits” all template for the industry and it has meant that the DNO systems have been consistently designed to the template. If the industry went away from that template then it would raise many issues for short term regulation and design but more importantly, we need to consider what the network will look like in 10-20 years if there was no minimum standard of compliance. DNOs indicated that it is clear that P2 has ensured that the networks in operation now have been built on solid foundations, without a standard, the network would be at risk from changing financial incentives as opposed to good engineering practice with a standard. It was also noted that P2/6 sets out planning standards in terms of large groupings of customers rather than individual customers.

DNOs reported that offering customers differing levels of security can prove difficult to manage on a practical and operational basis. To apply this strategy to all customers would require specific guidelines/rules to ensure that all parties were in agreement as to how to manage outages which would affect each customer. For class supply A-C the approach should be a planning standard which is prescriptive in the level of security required. Only individual large consumers can negotiate individual security levels, even then customers can only really choose their local connection security rather than the upstream security / redundancy. Such an approach may be acceptable for larger customers, but there would need to be arrangements to safeguard the reliability of supplies to the general domestic customer.

### Category 2 stakeholder responses

Respondents indicated that the existing (and revised) security standard should maintain the current emphasis relating to security of supply and not be side tracked by other issues.

It was also suggested by respondents that the existing document was applicable to all customers and in

<sup>11</sup> Class A group demand up to 1MW; Class B group demand Over 1MW and up to 12MW; Class C group demand over 12MW and up to 60MW, as presently defined in Engineering Recommendation P2/6.

all circumstances and they would not wish to see any dilution of the overall standard. They suggested that not all customers would be in a position or would wish to negotiate 'individual' security standards, while larger generators are able to negotiate (trade cost for security for example), smaller generators were likely to share their local network with other disparate users. In the latter case, common standards would seem more practical and appropriate. If network users could contract an enhanced security of supply, then the measures to achieve this would apply to some degree to others in the relevant Group Demands. Such "free riders" are unlikely to complain about their enhanced security of supply as it would be provided at no additional cost to them.

### Question 2.6:

Should the planning standard prescribe the (minimum) level of network security for smaller sizes of group demand (e.g. for class supply A-C) or should other regulatory incentives (such as IIS or other additional incentive mechanisms) be used that could provide a higher (incentivised) level of network security?

#### Category 1 stakeholder responses

There was some obvious overlap between this question and the responses provided for Q2.5. It was generally indicated by respondents that the IIS may change more frequently than a planning standard and that DNOs can react to changing IIS by rapid deployment of technologies such as remote control or automation, but network design has a much longer time horizon. It was noted that IIS reinforcements were generally undertaken at 11kV and below. Reinforcements at 33kV and above are usually as a result of compliance requirements stated in P2/6. The implementation of P2/6 on the network has left most primary substations (e.g. 33/11kV) with dual circuits or automatically switched alternatives, so the total loss of supply of primaries is not likely to contribute greatly to CI/CML figures. DNOs indicated that relying on IIS incentives for the security of this level of demand is likely to lead to a reduction in security.

There was also general agreement amongst DNOs that P2 should be retained as a minimum level of security and retain an incentive scheme to encourage the provision of enhanced security where this is viable.

#### Category 2 stakeholder responses

Respondents indicated that the existing standard provides a high incentive to ensure that supplies can be restored quickly and that the main focus of P2/6 provides a standard of service that is appropriate. They suggested that P2 should remain the base line document for security of supply and that any other additional incentive mechanism that a DNO may wish to employ should therefore be in addition to (and not as a replacement to) P2. It was also indicated that incentives may not give users certainty about the level of security which may be planned or maintained. A standard should give a clear specification and there should be significant penalties for failing to meet the standard.

### Question 2.7:

How do you understand how customers value security?

In planning your network and conducting cost-benefit analysis, what economic value do you place on improvements in reliability, i.e. the reduced risk of interruptions?

For example, do you specify consumer damage functions, or use more simplistic representations of

customer damage, such as the IIS incentive rates?  
How has the value placed on network security by customers been changing in recent years?  
How do you expect it to change in the future, e.g. due to developments such as the increased reliance of the heat and transport sectors on the electricity system?"

#### Category 1 stakeholder responses

In general, DNOs indicated that customers placed a high value on security of supply but it was hard to quantify by using existing metrics and there was no uniform method to evaluate the value of security. Also, customers value security of supply depending on both their location and supply type – i.e. domestic or commercial/industrial. Those living in rural areas will expect, due to experience, some level of interruption to supplies. As the majority of rural customers are domestic the impact of a fault will be less than if the customers were commercial/industrial – impact on productivity levels therefore potential financial losses. Urban customers have higher expectations of uninterrupted supplies and are more likely to complain about faults which result in loss of supply.

It was indicated that general security through the CI/CML mechanism has delivered strong security for existing customers and would suggest it is set at the right level, but could be improved. From an outage and post fault planning perspective the IIS rates and potential emergency and contingency times to restore customers drives DNOs decision making for contingency measures.

DNOs indicated that they believe as people become more reliant on electricity as their primary energy source they would become even less tolerant to faults that take them off supply for any length of time and so would hope more importance would be placed on the minimum security level customers should have through allowed network investment from the regulator. DNOs agreed that as stated in the question, in the future reliance on the electricity system to serve heat and transport demands is likely to increase the societal impacts of a loss of supply and correspondingly increase the VoLL<sup>12</sup>. Also, longer term there was an expectation of management of increasing levels of demand flexibility as well as increasing penetrations of embedded generation and energy storage.

It was noted from respondents that P2/6 does not currently make distinction between different classes of customer using damage functions of VoLL. The different classes of customer have varying dependency on electricity and are closely associated with location (city/urban/rural). It was indicated that IIS suffers the same failing in that it considers all CI and CML to be the same. If VoLL (or rather LoLP<sup>13</sup> and VoLL together) could be robustly ascertained that would be a good basis for departure from (but not necessarily an alternative to) a deterministic standard. Also identified by DNOs was the fact that customers do have the option to request higher levels of security, which are clearly detailed in our design standards however, minimum cost tends to be the main driver.

#### Category 2 stakeholder responses

No responses from category 2 stakeholders were requested or received for this particular question, which was aimed specifically at category 1 stakeholders.

<sup>12</sup> Value of Lost Load

<sup>13</sup> Loss of Load Probability

## Question 2.8:

Do you see any impact from the deployment of smart meters (SM) on network security planning standards?

### Category 1 stakeholder responses

In principle DNO respondents felt that the only potential impact of smart metering on network security planning standards would be in the better understanding and hence improvement of forecasting of the behaviour of customers. SM data could assist the DNO in demand forecasting and better the understanding of the daily load cycle within the demand group. However, DNOs indicated that it was likely that customer behaviour would be more complex to interpret and understand, potentially with the daily demand cycles being less repeatable as there may also be changes driven by commercial incentives. Overall, it was unclear to DNOs whether this would impact network security or ESQC standards.

It was noted from the responses that smart meters should increase the visibility of LV and HV networks and enable DNOs to take further actions to optimise their performance and SM would enable the adoption of innovative tariffs that could cause extra complexities which would need to be understood and managed. Also it was indicated by respondents that there will be a significant amount of information available from smart meters which brings new challenges including the practicalities of managing and using this volume of data and the data security issues. The full benefits from smart meters are unlikely to be available until the end of the roll out in 2020 leading to the thought that a P2/8 could be more dynamic based upon available data but it was not envisaged that smart meters should have a large impact on P2/7.

### Category 2 stakeholder responses

One stakeholder pointed out that potentially such smart technologies would allow for more interaction between consumer demand and network challenges. The technology also could permit more individually focussed customer service offerings, compared to the one size fits all they currently experience with their direct neighbours.

## Question 2.9:

What changes to the current RIIO framework, in your view, would better promote efficient levels of investment to promote security of supply?

### Category 1 stakeholder responses

It was noted from DNO responses that it is important that any regulatory framework has the flexibility to both promote security of supply and more general levels of efficiency in the design, operation and management of the distribution system and its impact on the wider GB system.

The clear response from the DNOs indicated that there is no option to change RIIO-ED1 so there is need to be cautions that any changes to P2 do not create a financial requirement which cannot be met under RIIO ED1.

There was some suggestion from DNO responses that as the same RIIO incentive rates apply to an individual domestic customer and commercial / industrial customer, that perhaps different rates should be applied to different categories of customer. One DNO indicated that we should consider the different values customers associate to continuity of supply rather than restoration (within a certain time)

following an interruption, different customer groups may value this differently.

#### Category 2 stakeholder responses

In general respondents indicated that the timescale for the benefits of investment to accrue is vitally important. It was suggested that for distribution networks to develop towards a "smarter" architecture investment may need to take place ten to twenty years ahead of real benefit to consumers and generators. The RIIO framework allows for 're-openers' in order to consider changes in the energy networks landscape as eight years is a long time during which no changes can be made to the planned expenditure of the DNOs. It was noted that RIIO should incentivise investment in grid capacity ahead of need to prevent the piecemeal reinforcements that often occur.

#### Question 2.10:

What impact (if any) does the IIS have on your system design?

What interaction is there between the planning standard and requirements specified by IIS?

#### Category 1 stakeholder responses

Some DNOs indicated that the IIS has significant effect on system design, whereas other DNOs indicated the effect was of a lower order. The cost of outages on the DNO leads the DNO to mitigate the risk at every opportunity, so for each circuit at HV and above there is a strong incentive to try to ensure that any first circuit outage can be resupplied via switching, preferably automatic as soon as possible. Further up the voltage levels customer numbers get even bigger; there is a driver to ensure that demand can be resupplied all year for second circuit outages. This is not necessarily affordable as there are no allowances for it, but there is a driver to look for overall efficiencies that can be re-invested in these areas. However, it was noted that the IIS does not specify any requirements, it is a pure incentive mechanism.

One DNO indicated that the Primary network design generally had very little to do with IIS and is mostly driven by P2/6, whereas 11kV design and below incorporates both IIS measures and P2/6 compliance, but IIS provides stronger incentives at 11kV and below. It was also recognized that P2/6 is focussed on demand while IIS is focussed on numbers of customers; hence IIS encourages DNOs to think more carefully about the implications for customers.

One DNO noted that IIS has incentivised investments in fault mitigation technologies such as automation and remote control. Whilst for a given outage this still results in loss of supply, supplies are quickly restored to healthy sections of the network minimising the impact in terms of CI and CML. IIS also incentivises operation response improvements since there is a diminishing return on network investment from corresponding incentive revenue.

#### Category 2 stakeholder responses

No responses from category 2 stakeholders were requested or received for this particular question, which was aimed specifically at category 1 stakeholders.

## Question 2.11:

In reforming P2/6, do you consider there is a need for consistency with the NETS SQSS that we should consider and if so, to what extent?

What other interactions do you see between P2/6 and other regulatory and industry codes?

Are there any specific conditions that should be included?

### Category 1 stakeholder responses

Respondents agreed that for both the security of supply requirements and assessment methodology there should be a transition between the distribution system and transmission system and that the consistent treatment of demand and generation across the boundary is important. It was indicated by one respondent that the boundary between electricity Transmission and Distribution is arbitrary; a sentence in the Electricity Act and that there was no engineering justification for the distinction or the disconnects at the T&D boundary, so that the SQSS should be changed as appropriate. Respondents indicated that the NETS SQSS is a little broader than P2/6 and covers both operational as well as planning standards. At present the operational aspects for a DNO are covered by IIS. IIS gives good levels of reporting and strong financial incentives which should remain in place. NETS SQSS has the advantage of stating specific standards for generation connection, the principle of which might be helpful to a DNO. It was argued by one DNO that there was no need for further consistency between the two (other than interfaces across GSPs<sup>14</sup>) as these standards are attempting to achieve two different things: NETS SQSS – system stability at a national level, P2/6 security of supply at a regional level. However, other DNOs indicated that consistency with the SQSS is essential, as otherwise National Grid would be operating to a different standard from the DNOs and conflicts would occur.

There was wide support from respondents for inclusion of elements of how NETS SQSS is structured that could be written into P2/7. The security of the distribution network should remain separate to the security of the transmission network. However, where the distribution network is required to support the transmission network, this should not be to the detriment of the distribution network and vice versa. One DNO indicated that a key requirement would be consistency among standards, conventions and incentives such that DNO behaviours are driven unambiguously towards their customers' best interests and DNOs can be confident of recovering their reasonably incurred costs.

### Category 2 stakeholder responses

Respondents indicated that a revised P2 could take some lessons from the role and scope of SQSS, including the differentiation of generators and other connections, in that generators and demand may have fundamentally different security requirements, noting that P2 is silent on security of supply to generators.

It was further suggested that there is already consistency with P2/6 in some tables indicating common standards were used in the composition of both documents. It was unclear if there was an advantage or disadvantage in the design standards as SQSS is more detailed than P2/6.

It was also indicated by respondents that other relevant regulations and codes (including G59 and G83) provide a rationale for P2 but do not provide specific direction. Therefore any revision of P2 should take care to look at other regulatory documentation to ensure that the appropriate standard of supply is provided and that it does not unduly hinder the operation of such services.

<sup>14</sup> Grid Supply Point

There was a view presented to indicate that the NETS SQSS did not reflect risk appropriately, so for example, the loss of two circuits is not constant, but varies with weather conditions, generation profiles and specific location within the network etc. so the SQSS should be more robustly linked to probabilistic risk and recognise the varying value of lost load. It should also incorporate additional investment specified by security services etc. under the Critical National Infrastructure arrangements.

### Question 2.12:

Should the planning standard explicitly consider extreme events?

If so, how should the standard cater for High Impact, Low Probability (HILP) conditions such as extreme weather or ICT failures?

#### Category 1 stakeholder responses

DNOs indicated that their networks generally perform well but when high impact events occur it is generally only recoverable due to interconnection left by historic system design and growth. Using customer numbers as a trigger for N-2 security enhancements maybe a good way to ensure large populations are not left exposed when things go wrong. It is clear that customers, industry and government are very critical if DNOs cannot recover supply to their customers quickly even if the DNOs have built a compliant network (reference storms of winter 13/14).

There was generally wide support by respondents for planning standards not to include extreme events; such events should be dealt with by alternative regulatory mechanisms.

Respondents generally agreed that there needs to be a wider discussion regarding the way to address HILP events. One DNO indicated that having a clear understanding of what flexibility designs constructed under current infrequent contingencies would provide in respect to HILP is clearly valuable and would necessarily involve co-ordination across industry parties. In general there is limited cost benefit for inclusion of HILP mitigation in the design stage and in general the response approaches to HILP would normally most optimally sit outside of those considered under BAU; that is consideration of exceptional events would not be consistent with the design of a techno-economic network.

Some respondents argued that it would be difficult to identify/agree a common set of rules that could apply equally to DNOs without major differences in investment to seek compliance; however, some potential mitigations could be included in any new standard.

DNOs indicated that if it is decided that all customers and society as a whole accept the risk of extreme events, (e.g. impact on the local and national economy) then such risk should be excluded from the IIS framework. One DNO suggested that P2/6 did cater for HILP risks, at least to some extent, by requiring redundancy.

Although the DNOs did not necessarily see failure of IT systems as a HILP event, it was noted that as the system becomes more heavily dependent on IT and communications infrastructure, risks associated with failure of these assets needs to be included in the security assessments.

#### Category 2 stakeholder responses

In general respondents agreed that the current arrangements for HILP being outside of the P2 standard

were appropriate and they should be maintained. It was suggested that any deviation away from the current arrangement would add confusion to what is a very simple and effective security planning method and would add little if any value to the overall document.

### 3.3 SECTION 3: Real time Network Operation and security of supply

It should be noted that the questionnaire was designed to elicit feedback and thoughts regarding the real time operation of the system. Specifically, views were sought regarding the changes in real time network operation and control that could be facilitated through new software applications and supporting ICT infrastructures that will be available to facilitate the transition to a "smart grid" paradigm, with a specific focus on the impact on security of supply. This section was only included in the discussion to gain views on different aspects of the application of IT and real time operation. The questions were not directly related to the security standard but used to supplement and expand some of the detailed quantitative analysis. For this reason, the questions have been included in this report, (for transparency) but none of the responses from any party have been included in this report as they have been used to supplement the analysis undertaken by Imperial College.

#### Question 3.1:

What are your experiences of the impact on security of supply as a result of changes in real time network operation and control in support of the deployment of "smart" devices on the network?

#### Question 3.2:

To support the move towards a "smarter" network, what Information and Communications Technology (ICT) infrastructure have you developed, or plan to deploy, on the network to have an (positive) impact on the security of supply?

#### Question 3.3:

What experience have you gained and (any) lessons learnt from real-time system control (including supporting ICT requirements) relating to system security, from LCNF projects and/or any other associated pilot studies or trials?

Please provide any relevant example project references that we may investigate further.

### 3.4 SECTION 4: Additional Questions and points for consideration

Stakeholders were asked if there any additional points that they believe should be considered during the analysis phase of the project or included in the wider review?

These may include:

- Transparency and practicality of the future standard.
- Acceptability and application.
- Others related issues.

#### Category 1 stakeholder responses

There was general feedback from respondents to indicate that the eventual solution to any replacement/update to the security standard should be an evolution of the existing standard and be:

- Clear and transparent for all users (that is NOT a “black box” approach)
- Capable of supporting/elaborate upon investment cases where investment was likely to be contentious i.e. in establishing new 33kV or higher voltage routes.
- Practical and straight forward to implement
- Capable of supporting current non-network technology and future network technologies

There were some comments, from the DNOs (not directly related to the security standard) indicating that there was also a need for coordinated TO/DNO planning in many areas going forward including embedded generation, DSR and outage planning.

#### Category 2 stakeholder responses

Respondents were of the opinion that Electricity Distribution is a nationally critical infrastructure, both for all network users and for new consumers and generators (to support the future or growing economy) and that economic growth usually necessitates modification to electricity distribution infrastructure to act as an enabler. It was suggested that some linkage between DNO investment and regional or local planning policy or designated economic development areas would benefit the UK economy as a whole.

Stakeholders supported the view that the current format of P2 provided a good level of transparency, practicality and that such a level of certainty must be maintained.

It was highlighted by respondents that distributed generation (DG) projects must now be considered to be a normal connection arrangement and therefore must be included within any P2 revision such that DG projects/connections receive a suitable and defined level of security of supply.

It was also noted by some respondents that the planning standard is an industry wide standard and potential policy changes in the future may enable a more liberalized connection regime, in which case the security standard should be designed in such a way that any Planning Engineer would be capable of interpreting it without reference to any complex analysis, DNO support or technology specific arrangements.

## 4 STAKEHOLDER VIEWS ON THE FUTURE SECURITY STANDARD - HIGH LEVEL OPTIONS.

Please note that this chapter summarises statements and opinions expressed by respondents as detailed in section 3, which should not be taken to represent the views of the consortium or DCRP P2 working group.

### 4.1 Developing a better understanding of P2/6 strengths and weaknesses

Network Owners and operators are obliged to plan and operate their networks in an efficient, economic and coordinated manner and most respondents to our questionnaire expressed the opinion that this has been largely supported and guided by the existing P2 standard over the years. Many respondents commented that P2 has complemented licensees' activities in a clear, robust and auditable manner which has not only supported a broadly consistent planning approach across organisational boundaries but provided a basis by which customer requirements may be easily articulated, and their supporting need for consent and investment demonstrated.

The following section provides a summary of the responses and more detailed discussions with all stakeholders to summarise their views on the strengths and weaknesses of P2/6, and potential improvements.

#### **Efficiency and Security of Supply**

Respondents generally agreed that the current standard provides definitive guidance to security of supply arrangements and many expressed a desire that these arrangements be continued and remain the focal point of any revised or updated standard, and noted the benefits of the current standard's clarity and transparency. Some suggested that it would be desirable to retain standards for demand type connections and to supplement the document with agreed standards for distributed generation connections.

Further, many respondents told us that P2/6 and its predecessors have always sought to be rationally based, evaluating investment cost and risk on a probabilistic basis, rather than the more simple deterministic (and arguably less demonstrably economic) transmission standards. A future P2 would need to incorporate additional flexibility to cater for a more widely divergent customer base and also enable DNOs to plan more strategically – for example by investing ahead of need, when the longer term economics suggest that this is a less costly option.

On balance, the majority of respondents told us that they consider that the design standard was generally efficient, but offered little evidence to support this position. Further, as all GB DNOs have developed networks in accordance with the same guidelines it is now difficult to form a view of whether the GB system performance / cost are efficient or inefficient. Nonetheless, there was general agreement that P2/6 does seek to balance the cost of loss of supply against network assets, even if it requires updating in some respects. In particular, most respondents supported the case for a review of P2/6 at this time as the standard is based on 1970s figures, both costs and values, so the value of lost load in P2/6 will probably be understated, whilst the costs are probably too expensive in real terms.



For generation customers, however, responses indicate some disjoint between expectations around security and what P2/6 delivers. However, generators are resistant to providing any greater level of funding for the enhanced security they believe they should receive.

It is clear that Security of Supply and Electrical Losses are two different objectives for which DNOs need to account for when planning their networks. Many respondents supported retaining the main focus of the security standard on minimum design standards for different levels of demand, and to avoid duplicating any obligation to consider losses as part of the overall objective to deliver an economic and efficient network.

### **Whole life costing**

The view from the DNOs is that while P2/6 does not strictly require them to take “whole life costing” into account this does not imply that networks were designed without due consideration for cost minimisation. However, some respondents indicated that a formal requirement should be included in the replacement security standard to ensure that efficient network design and investment is central to the future of network development. Discussions with respondents indicated that DNOs have no single definitive definition of “whole life costing”, by the DNOs

### **Treatment of construction outages**

From the questionnaire responses and discussions, it is clear that DNOs treat management of construction outages differently to fault conditions. They prioritise the mitigation of faults during planned outages based on the potential financial impact and the reputational impact on them. It was generally stated that construction risks were often viewed as being more controllable by the DNOs as there is the opportunity to plan and evaluate mitigation measures. Part of the risk mitigation approach identified was to plan construction outages during a period where the network was under less stress and more amenable to reconfiguration and switching, so construction outages are almost always scheduled for periods of lower demands to minimise risks. However, it was recognised that while this has worked well in the past it may be more problematic in the future to accurately determine such periods. Possible future changes in customer behaviour and demand patterns may mean that predicting a season when the network was less stressed may not be possible (or at least more difficult) leading to greater uncertainty when planning long term construction outages.

### **New-network technologies and arrangements to aid network security**

One of the significant omissions of the existing standard, and a key area for a potential reform identified by respondents, is the treatment of non-network technologies and commercial arrangements that are under development and able to provide non-traditional methods to increase network capacity and performance. These include (but are not limited to) energy storage devices, DSM, DSR and other commercial arrangements, that are at different stages of maturity in development and in some cases approaching roll out status in the UK. It is important that such devices and arrangements are accounted for in forming any new ER to enable them to be part of the network design process and provide their range of services to the market and the network. This will enable the future network work design to consider the benefits that are provided by such devices with a view to fully utilising their capabilities to maintain the required level of security while minimising the cost of such services to the network operator.



Some respondents indicated that network attached devices that are able to deliver network operational support services should expect the same level of connection security and transparency as provided for demand customers, including the same level of restoration times. Whilst, restoration times are not in the scope of this project, some stakeholders indicated that restoration times should be the subject of wider industry discussion and debate and at the earliest opportunity. It was noted that in principle, storage and DSR/DSM have a very different set of operating characteristics to those of the traditional network assets and some are dependent on the behaviour of customers. Although they are controllable, a number of respondents indicated that unless the DNOs are able to persuade customers to behave in a way that supports the local network operation, their potential benefits may not be achievable and indeed may have a detrimental effect of the network.

Stakeholders were all in agreement that distributed generation (DG) projects must now be considered to be a normal connection arrangement and therefore must be included within any P2 revision such that DG projects/connections receive a suitable and defined level of security of supply.

Responses to our questionnaire, and the subsequent discussions, suggests the **strengths** of the Engineering Recommendation include:

- The ER in its current version has stood the test of time and underpins fairly good system performance;
- Short , clear and easy to understand and implement;
- Implements probabilistic assessments in a deterministic manner;
- Increases the required network resilience with increase in demand / number of customers;
- Provides resilient networks that cater for a wide range of contingencies especially for large load groups;
- Simple for all stakeholders (ranging from government/regulators to customers) to understand and interpret;
- Sets out a long term clear minimum standard required for the networks to meet (or exceed if required);
- Provides a common framework for price control baseline;
- Well understood and aligned to current design practice, forms the basis of DNO planning methods, and
- Assumes a top down flow of energy and places the greatest resilience at the top levels.

Similarly, the **weaknesses** of the Engineer Recommendation, based on our stakeholder discussions and reviews were identified as:

- Does not imply the necessary level of network performance at lower levels (11kV and below), IIS tends to require a greater level of security than prescribed by P2/6, but is only an incentive mechanism rather than a design standard;
- Does not include statements or treatment of DSM, generation, storage, other network solutions (smart grids) or provide a degree of "future proofing" for new technologies but must be realistic when considering the levels of security offered and relied upon;

- Does not consider the security of the connection between the generation point of connection and the network when assessing the security contribution from that generation or provided to the generator;
- Does not make provision for real-time considerations which will become more prevalent as smarter technologies and more flexible, controllable and variable load are more widely adopted within GB distribution networks;
- There was some concern that long term investment is not adequately supported and that early investments to offset later and wider reinforcements were not well supported;
- The requirements and forecasting for demand groups <1MW should be better and clearly defined and the derivation of "circuit capacity" may be inconsistent;
- Assumes all customers value electricity equally at all times and probably at a rate that understates modern expectations which is likely to increase into the future;
- Does not cater for the frequency of interruptions;
- Does not consider circuit length, routing or type of terrain;
- Assumes that all maintenance outages are for a short term duration, which may not be the case, there is a lack of clarity on what maintenance period is allowed, some outages are permitted for (unlimited) repair time;
- There is some ambiguity in terms or lack of definitions of terms which can lead to different interpretations of the standard
- There is a lack of clarity on whether certain fault conditions are included in the standard, this should be addressed, including busbar faults (which are not inherent in the design standard);
- There appears to be a bias as the ER provides some statements regarding DG but none for DSR.

The discussions and analysis of the stakeholder responses also produced some suggestions on potential **features and improvements** any new security standard could provide and included:

- Consistency with the existing regulatory framework and future changes;
- Be simple / easy to apply, with unambiguous statements and consider the availability and cost of planning staff required to apply a methodology;
- Sufficiently intuitive and easy to audit;
- Easy to explain in public enquiries, disputes and/or way leave hearings;
- Facilitate efficient investment / demonstrate ESQC compliance;
- Introduction of and clarity in the use of "whole life costing" and use of NPV cost minimisation supported by a clear definition of the terminology, to ensure networks are designed with more focus on long term efficient design and investment and central to the security standard;
- Flexible and open to align with, or accommodate regulatory incentives, including IIS;
- Reflect network user expectations / customers willingness to pay for levels of security and meet their requirements as they evolve;

- Treatment of network losses should not be included in the standard but the interface between other industry standards/regulatory initiatives should be enhanced to ensure that the incentives exist and correctly work in conjunction with the security standard, rather than against each other.
- Prescriptive enough to ensure all DNOs are designing to the most economically efficient and common sets of methods to provide supply of security that offers the best value for customers but also balanced with adaptability to facilitate new/innovative methods of managing the network / network demand.
- Inclusion of management of construction outages and methods to minimise risks.
- Inclusion of a definition of Firm Capacity;
- DSR must be introduced into the document and treated in a clear and robust manner, and
- Full and clear balanced representation of DG / DSR / storage and other network technologies.

## 4.2 Alternative approaches To Security Standards and Regulatory and commercial considerations

### General Approach

Respondents generally agreed that any revision to P2 should take into account the contribution to security of supply of new non-network technologies, including (but not limited to) energy storage and DSR that are approaching roll out in the UK. Providers of these services suggested they would expect the same level of clarity and transparency of security and robust network design and reliability as enjoyed by demand customers.

It is important to note that in principle storage and DSR/DSM are controllable, however, unless the DNO is able to persuade customers to behave in a way that supports distribution network operation, their potential benefits may not be achievable. In a market based system this means that DNOs have to be able to procure certain services from customers but this must be completed in a fair and equitable manner across all customers.

Clearly, DNOs will need to understand the reliability and availability of non-network technologies to deliver security services to the network, not all DSRs have the capability to provide the same level of response or reliability to deliver, so methodologies to identify the extent of DSR effectiveness on network design would need to be identified. In support of this service provision, there would need to be a robust assessment of the contribution that contracted services could make to the network and the level of security that could be provided, but some respondents suggested it should be left to the DNO to quantify these contributions perhaps through the use of reliability factors rather than prescribed by the standard. Respondents accepted that, where the DNO has direct control of the demand, then this may have a clearer contribution to security but there were still many variables for security risk that must be taken into account.

### Should we move to a CBA based standard or should P2/6 be removed?

A potential option under investigation is to replace the P2/6 standard by an obligation to perform stochastic cost-benefit analysis when planning the network, if this was to be the case there is potentially



a requirement for Ofgem to provide additional oversight and an approval mechanism for such an approach. Some respondents raised concerns regarding the practicalities and additional costs of carrying out a stochastic assessment for each HV and EHV scheme, suggesting there would need to be a prescriptive approach for at least the most common studies, and that quantifying the benefits to customer groupings would be challenging in some cases. In addition, some respondents felt that agreement would be required on the risk assessment process and parameters to ensure consistent application, and that this would require inputs from Ofgem to support development of, and ultimately approve, the methodology. Some respondents also noted the need for oversight of any obligation to conduct CBAs to ensure DNOs make the economically efficient choices in respect of the degree of Supply Security provided to customers, making appropriate use of new/innovative methods of managing the network / network demand.

Some DNOs raised concerns regarding the time and resource impact on their planning departments and that Ofgem may become more involved with network designs, which is not practical or feasible given the level of resources available to all parties. However, there was general support for the adoption of CBA modelling by DNOs and Ofgem to further inform decision making and it was viewed as a positive move so long as the decision making framework was only one component of the overall process.

Another option is to remove the security standard completely and use other applicable regulations, such as the IIS, to encourage efficient levels of investment to ensure security of supply. Most DNOs said this change would not affect their planning decisions for Group Demands below 100MW and the IIS incentive drives system design at these lower demand levels, to ensure that losses of supply are minimised both in number and duration. However the IIS incentive could be altered or removed by Ofgem and it does not constitute or seek to replace a design standard.

Some DNOs noted the broad obligation to “Plan and develop the distribution system in accordance with a standard not less than that set out in Engineering Recommendation P2/6” (a requirement under the Electricity Act). Removal of a formal planning standard may enable DNOs to focus on other drivers, such as CI/CML benefits. But DNOs’ responses to such a change in regulation might vary.

Through the questionnaire, and subsequently in discussions with respondents, we sought comment on the hypothesis that planning standards are not required if network users can contract for the degree of security of supply they want. For instance, some consumers can already negotiate with the DNO regarding the “firmness” of their connection, making a trade-off between cost and the degree of security they purchase. In response, most comments suggested it was difficult to understand how smaller customers would be in a position or would wish to negotiate their ‘individual’ supply security, while larger generators are able to negotiate smaller generators are likely to share their local network with other disparate users. In the latter case, common standards would seem more practical and appropriate. If network users could contract for enhanced security of supply, then the measures to achieve this could apply to some degree to others in the relevant Group Demands.

## **Valuing Security**

The efficient level of security depends on a trade-off between the level of reliability provided and the cost of the provision. Hence, our questionnaire asked how DNOs viewed the value customers place on security.



In general, DNOs indicated that customers placed a high value on security of supply but it was hard to quantify this using existing metrics and there was no uniform method to evaluate the value of security. Also, customers value security of supply depending on both their location and supply type. There was a general feeling that as people become more reliant on electricity as their primary energy source they would become even less tolerant to faults that take them off supply for any length of time and so would hope more importance would be placed on the minimum security level customers should have through allowed network investment from the regulator. Also as the future reliance on the electricity system to serve heat and transport demands is likely to increase the social impacts of a loss of supply and correspondingly increase the VoLL. In the longer term, the value of security may also be affected by factors such as increasing levels of demand flexibility and increasing penetration of embedded generation and energy storage.

### **Interactions with other industry documents**

Some respondents noted that P2/6 is part of a fully integrated set of industry based documents that provide interactions and dependencies across the delivery chain, from transmission connections down to the end user customers. They suggested that interactions with other documents are taken into account and some suggested there is a need to maintain or update any links between the standard and other documents. Some suggested that for both the security of supply requirements and assessment methodology there should be a transition between the distribution system and transmission system and that the consistent treatment of demand and generation across the boundary is important. The boundary between Transmission assets and Distribution assets is arbitrary, defined by a provision in the Electricity Act. There is no real engineering justification for the distinction or the disconnects across the boundary.

The NETS SQSS is a little broader than P2/6 and covers both operational as well as planning standards. At present the operational aspects for a DNO are covered by the IIS which provides good levels of reporting and strong financial incentives which should remain in place. The NETS SQSS has the advantage of stating specific standards for generation connection, the principle of which might be helpful to a DNO. Potentially the two security standards are attempting to achieve two different things: NETS SQSS – system stability at a national level, P2/6 security of supply at a regional level so there is no need for further consistency between the two (other than interfaces across GSPs). However, it would seem sensible for a high degree of consistency between them to exist otherwise National Grid would be operating to a different standard from the DNOs and conflicts would occur. The key requirement would be consistency among standards, conventions and incentives, and ensuring that DNO behaviours are driven unambiguously towards their customers' best interests and DNOs can be confident of recovering their reasonably incurred costs.

### **Extreme Events**

Our questionnaire elicited views on the options for how High Impact, Low Probability (HILP)<sup>15</sup> events should be accounted for in any new standard. DNO networks generally perform well but when high impact events occur it can be that supply losses are only recoverable due to interconnection left by historic system design and growth. It is clear that customers, industry and government are very critical if supplies to customers are not quickly recovered even if the network is fully compliant. There was

---

<sup>15</sup> High impact low probability events can be where multiple or common mode faults or failures impact on the network outside of the designed security arrangements and where the supply loss impacts many customers or high profile customers. The reason why designs may not cater for such events is that they are assessed to be very unlikely to happen or difficult to predict and the mitigation costs are potentially very high. Rather than design networks to cater for HILP, operators may consider how they respond to such events.



general agreement for planning standards not to include extreme events; such events should be dealt with by alternative regulatory mechanisms due to their low probability.

In general DNOs were of the view that there would be limited (cost) benefit to support the inclusion of such events in the design stage and any response or approaches to HILP would normally sit outside of those considered to be BAU. There was general agreement amongst respondents that there needs to be a wider discussion regarding the way to address HILP events outside of the P2 review. Some respondents viewed that it is difficult to understand how the planning for, and management of exceptional events would be consistent with the design of an economically efficient network as it would be difficult to identify/agree a common set of rules that could apply equally to all networks under all circumstances without major differences in investment to provide compliance.

## 5 SUMMARY OF STAKEHOLDER VIEWS

From the analysis of the various stakeholder questionnaire responses and details of the clarifications gathered by stakeholder interviews, the following themes emerged relating to the reform of P2/6. There is no prioritisation stated or intended in this list, as respondents were not asked to provide a view as to the level of importance relating to the potential standard updates or replacement strategies. Some updates are only directly relevant to specific stakeholder groups; however, a number of key themes were identified by the majority of stakeholders:

**Embrace the strengths of the existing standard** – a strength of the existing standard is its simplicity. Many respondents (from both categories<sup>16</sup>) suggested this simplicity and transparency should remain to ensure the usability of any future standard. Respondents suggested that any new sections should be clear and concise. Any new obligations placed on DNOs to undertake more complex planning exercises should consider the availability and cost of planning staff required to apply the new standard methodologies.

**Provide consistency with the regulatory framework** – the new standard should be developed in such a manner that it is consistent with the existing regulatory framework and flexible enough to adopt potential future changes without a major review of the regulatory system. The new standard will need to align with, or accommodate regulatory incentives, including the IIS. Some respondents discussed the possibility of delaying implementation of any new standard that imposes new obligations on DNOs until the start of the next price control period.

**Remain sufficiently intuitive and easy to audit** – Some respondents noted as a benefit of the existing standard the ease with which it can be explained in legal proceedings, such as way leave hearings or disputes, which can minimise dispute costs and delays. Further, it helps DNOs to demonstrate ESQC compliance.

**New network technologies must be fully represented** – it is clear from all parties that the revised standard must consider both demand and non-demand sites and other network technologies. This should include (but are not limited to) energy storage devices, DSM, DSR and other commercial arrangements. It is important that such devices and arrangements are included in the standard to enable them to be part of the network design process and provide their range of services to the market and the network. This will enable the future network work design to consider the benefits that are provided by such devices with a view to fully utilising their capabilities to maintain the required level of security while minimising the cost of such services to the network operator.

**Provide a clear and consistent set of definitions** – some of the existing P2/6 statements are open to interpretation which leads to different views being formed of some of the statements and requirements, all terms in any new standard ought to be comprehensively and clearly defined, including the inclusion of a definition of Firm Capacity (if this term is used in any new standard).

**Reflect network user expectations** – the new standard should fully reflect all network user expectations (both demand and non-demand), be able to include customer willingness to pay for levels of security and meet their requirements as they evolve in the future.

---

<sup>16</sup> Category definition of respondents defined in section 2.3.



**Introduction of Cost Benefit Analysis** – there is general support for the use of CBAs in the new standard to help inform decision making and guide optioneering but only as one component of the overall process and the method should be used within a closely defined context.

**Treatment of network losses should not be included** – Most respondents took the view that the security standard should not be adjusted to explicitly consider network losses, but suggested that the interface between other industry standards/regulatory initiatives should be enhanced to ensure that any incentives work correctly in conjunction with the security standard to support its intent of ensuring the efficient provision of security of supply.

**Statements of requirements should remain prescriptive** – Many respondents took the view that the description of the requirements imposed by the planning standard should be prescriptive, ensuring all DNOs are designing to the most economically efficient and stated common sets of planning methods. This will provide a level of supply security that offers the best value for customers but also balanced with adaptability to facilitate new/innovative methods of managing the network / network demand.

**Include the management of construction outages** – Some respondents expressed a desire for the new standard to provide guidance as to the methods for the treatment of construction outages that will provide a more consistent approach for all DNOs to adopt and provide consistency across networks. This will become increasingly important as the shape of the network demand becomes more difficult to forecast as the penetration of new LCT increases and DNOs will have less choice of when to minimise the risk associated with a construction outage.

**Treatment of Extreme events** – extreme events (as characterised by HILP (high impact, low probability)) should not be included in the new/ revised standard. Such events should be treated within the regulatory framework. It was noted that a wider debate (which is outside the scope of this project) should be initiated across the industry to agree the most efficient way to treat such events.

As in previous chapters, please note that the views summarised above are those of the respondents. Statements made by respondents should not be taken to represent the views of the consortium or working group. .



## **APPENDIX A      INDUSTRY QUESTIONNAIRE.**

Appendix A includes details of the various sections from the industry questionnaire including the guidance for completing the questionnaire and all questions. The industry questionnaire was supplied to all participants listed in Appendix B.



## Table of contents

1	INTRODUCTION.....	1
2	QUESTIONNAIRE .....	3
3	SECTION 1 - DEVELOPING A BETTER UNDERSTANDING OF P2/6 STRENGTHS AND WEAKNESSES .....	10
4	SECTION 2 -ALTERNATIVE APPROACHES TO SECURITY STANDARDS AND REGULATORY AND COMMERCIAL CONSIDERATIONS .....	17
5	SECTION 3: REAL TIME NETWORK OPERATION AND SECURITY OF SUPPLY.....	28
6	SECTION 4: ADDITIONAL QUESTIONS AND POINTS FOR CONSIDERATION.....	28
7	CONTACTS.....	16

# 1 INTRODUCTION

In January 2014 the Distribution Code Review Panel<sup>17</sup> P2 Working Group (DCRP P2 WG), through the Energy Network Association,<sup>18</sup> (ENA) engaged a consortium comprising DNV GL<sup>19</sup>, Imperial College London (ICL)<sup>20</sup> and NERA Economic Consulting<sup>21</sup> (the Consortium) in a project to carry out a full “back to basics” review of Engineering Recommendation P2/6.

The requirement for a fundamental review of Engineering Recommendation P2 has been recognised by Network Licensees (i.e. the Electricity Distribution Network Operators (DNO) companies and National Grid) for some time. The Licensees therefore believe that it is timely to undertake a comprehensive review of Engineering Recommendation P2 in relation to customer and system requirements and to develop an understanding of what is required to facilitate the long term development of networks.

The fundamental review of ER P2/6 is being directed by the Distribution Code Review Panel P2 Working Group (DCRP P2 WG) through the Energy Network Association (ENA).

The review will be performed in two distinct phases. **Phase 1**, which is programmed to be completed around March 2016, is essentially a comprehensive research, analysis and modelling engagement and consultation process carried out by the Consortium with direction and support provided by the DCRP P2 WG and the ENA. Network licensees have no preconceived approach to future security standards. The spectrum of possibilities ranges from a modification and update of the current arrangements, development of a completely new approach starting from first principles, through to recommending removal of any deterministic planning standard, relying instead on the DNOs’ regulatory incentives and other legislation to motivate efficient network design. The Consortium will complete their evaluation of these agreed options, conduct a programme of industry engagement, including formal industry consultation, and recommend the most appropriate approach that should be taken forwards into **Phase 2** and codified.

A key part of Phase 1 is to gain a detailed understanding of the position of the many stakeholders as a starting point for our analysis. The most effective way to understand the current status and thoughts of the industry is through feedback directly from the stakeholders, so the Consortium is conducting a series of structured interviews, based on this questionnaire, with a variety of different parties. These interviews are designed to support the review analysis activities, particularly the qualitative analysis, and to ensure that relevant industry participants have had significant input into the final output. As far as the DNOs are concerned, we envisage that interviews will be conducted with those setting planning policy, operational engineers (i.e. those that have experience of operating the network or managing outages), Future Networks teams (i.e. those looking at future

- 
- 17 The Distribution Code Review Panel (DCRP) is the body responsible for overseeing the maintenance and development of the Distribution Code and its subordinate documents. Those subordinate documents include Engineering Recommendation P2/6. The ENA is the service provider to the DCRP for the physical maintenance of the Code and its subordinate documents.
  - 18 Energy Networks Association is the industry body for UK energy transmission and distribution licence holders and is the voice and agent of the energy networks sector. ENA acts as a strategic focus and channel of communication for the industry and aims to promote the interests, growth, good standing and competitiveness of the industry. They also provide a forum for discussion among company members, and so facilitate communication and sharing of experience across the energy networks sector
  - 19 DNV GL is a Global certification and advisory business working in the maritime, oil and gas, business assurance and energy sectors.
  - 20 Imperial College London is a university of world-class education and research in science, engineering and medicine, with particular regard to their application in industry, commerce and healthcare.
  - 21 NERA Economic Consulting is a global firm of experts dedicated to applying economic, finance, and quantitative principles to complex business and legal challenges.



developments and new technologies) and regulatory/commercial teams (i.e. those concerned with interactions between P2 and the regulatory settlement, as well as other aspects of DNOs' licences and other industry codes, as well as the financial impact of any change.

The purpose of this questionnaire is to gather experience and comment from different sources so that relevant information, current practices and future views can be identified and utilised during P2 review process. Representatives from each of the DNOs will be interviewed, using this questionnaire as a structure. While the consortium would prefer direct face to face interviews, due to the geographical spread of stakeholders, interviews will be through a combination of direct interviews and teleconferences based around the three geographic areas identified in this document.

We would ask each party to complete the questionnaire prior to the arranged interview using the "Response" section in each case, so that the Consortium interview team are able to discuss your responses. Any additional comments will be added in "Additional Comments" as an outcome of the interview.

## 2 QUESTIONNAIRE

The remainder of this document sets out a series of questions for completion, seeking general and detailed comments and feedback (as appropriate), divided into four subject areas:

- **Section 1** - Developing a better understanding of the strengths and weaknesses of ER P2/6;
- **Section 2** - Alternative approaches to Security Standards and Regulatory and Commercial considerations;
- **Section 3** – Real time network operation and security of supply, and
- **Section 4** - Additional questions and points for consideration.

All responses provided will be used to support our initial analysis, so please make the responses as detailed as possible and include supporting evidence or relevant examples where necessary. Each table in the following sections present a question, (or set of related questions around a specific topic area) that should be addressed. There is an area in each table for the “Response” that should be completed as fully as possible prior to the interview. The “Additional Comments” section will be completed after the interview to capture other elements of the discussion.

At present all responses will be treated as confidential and will not be disclosed to any third party. There may be some merit and benefit in sharing the responses with other companies either named or anonymously. For each question, please indicate your preference as detailed below:

- Keep response anonymous (the default).
- Share the response but without reference to company or project.
- Share the response with other respondents.

### 3 SECTION 1 - DEVELOPING A BETTER UNDERSTANDING OF P2/6 STRENGTHS AND WEAKNESSES

In this section of the questionnaire, we seek views and feedback to aid a clearer understanding of the (perceived) strengths and weaknesses of the existing security standard.

<b>Question 1.1:</b>
Is the present network design standard efficient? Does it deliver value for money to all network customers? In other words, does it balance the cost of network infrastructure with the security benefits delivered to distribution network customers?
<b>Response:</b>
<b>Additional Comments:</b>
<b>Response Status (please indicate):</b>
<input checked="" type="checkbox"/> Response to remain anonymous (default). <input type="checkbox"/> Share the response but without reference to company or project. <input type="checkbox"/> Share the response with other respondents willing to share their information

<b>Question 1.2:</b>
What, in your view, what are the strengths and weaknesses of P2/6? How might it be improved? What should be the key features of the new security standard (if required)?
<b>Response:</b>
<b>Additional Comments:</b>
<b>Response Status (please indicate):</b>
<input checked="" type="checkbox"/> Response to remain anonymous (default). <input type="checkbox"/> Share the response but without reference to company or project. <input type="checkbox"/> Share the response with other respondents willing to share their information

**Question 1.3:**

How does “whole life costing” impact on the planning/designing your network?  
Do you feel that “whole life costing” is adequately captured within P2/6?

While there is no single definitive definition of “whole life costing”, we would like to understand the cost components considered by each DNO. For the purposes of responding to this question, the working definition of “whole life costing” would be: “the systematic consideration of all relevant associated costs of network assets, including: construction, ownership and maintenance”.  
We are also interested in costing definitions which may be provided in the response.

**Response:**

**Additional Comments:**

**Response Status (please indicate):**

- Response to remain anonymous (default).
- Share the response but without reference to company or project.
- Share the response with other respondents willing to share their information

**Question 1.4:**

We are aware that DNOs treat construction outage management differently to fault conditions. How do you quantify the increased risks of customer interruptions associated with long term construction (or maintenance) outages?

**Response:**

**Additional Comments:**

**Response Status (please indicate):**

- Response to remain anonymous (default).
- Share the response but without reference to company or project.
- Share the response with other respondents willing to share their information

**Question 1.5:**

In your view, should the planning standard include an explicit requirement for DNOs to account for the loss inclusive network design?



Do you have any suggestions regarding the form that such a requirement should take?

**Response:**

**Additional Comments:**

**Response Status (please indicate):**

- Response to remain anonymous (default).
- Share the response but without reference to company or project.
- Share the response with other respondents willing to share their information

## 4 SECTION 2 -ALTERNATIVE APPROACHES TO SECURITY STANDARDS AND REGULATORY AND COMMERCIAL CONSIDERATIONS

In this section of the questionnaire, we seek views and feedback regarding potential alternative approaches to the existing (and any future) security standard and the impact of Regulation and commercial propositions on the security standards

### Question 2.1:

If P2/6 were enhanced to account for non-network technologies (e.g. storage and DSR/DSM), what types of changes to the existing standard do you think could be implemented to achieve this, and what are the advantages and disadvantages of these alternatives?

### Response:

### Additional Comments:

### Response Status (please indicate):

- Response to remain anonymous (default).
- Share the response but without reference to company or project.
- Share the response with other respondents willing to share their information

### Question 2.2:

Technologies such as embedded generation, storage and DSR/DSM may behave in a way that is supportive to the distribution system (e.g. in response to time of use distribution tariffs), or they may behave in a way that is supportive to the power system as a whole (e.g. in response to power price signals). Should this issue be included in system planning and if so, how?

### Response:

### Additional Comments:

### Response Status (please indicate):

- Response to remain anonymous (default).
- Share the response but without reference to company or project.
- Share the response with other respondents willing to share their information



**Question 2.3:**

Supposing that P2/6 were replaced by an obligation to perform stochastic cost-benefit analysis when planning the network:

- How prescriptive do you think such an obligation would need to be in terms of specifying the modelling approach and assumptions that should be used for such studies and the options that they should consider?
- What process of oversight/approval by Ofgem would you consider necessary/proportionate? For instance, scheme-by-scheme approval/audit, approval of DNO-specific or industry-wide modelling tools/modelling methodology statements?

**Response:**

**Additional Comments:**

**Response Status (please indicate):**

- Response to remain anonymous (default).
- Share the response but without reference to company or project.
- Share the response with other respondents willing to share their information

**Question 2.4:**

How do you believe your/DNOs' asset planning policies would change if P2/6 were removed entirely?

What are the pros and cons of removing P2/6 completely?

Absent P2/6, would the current suite of outputs obligations and financial incentive mechanisms implemented through RII0-ED1, as well as any other applicable regulations that affect your asset planning, be sufficient to encourage efficient levels of investment to ensure security of supply?

**Response:**

**Additional Comments:**

**Response Status (please indicate):**

- Response to remain anonymous (default).

- Share the response but without reference to company or project.
- Share the response with other respondents willing to share their information

**Question 2.5:**

We are exploring the hypothesis that planning standards are not required if network users can contract for the degree of security of supply they want. For instance, some consumers can already negotiate with the DNO regarding the “firmness” of their connection, making a trade-off between cost and the degree of security they purchase:

- Should the planning standard prescribe the amount of network capacity for smaller sizes of group demand (e.g. for class supply A-C)?
- Should the planning standard prescribe the amount of network capacity provided for generators, given that they can negotiate with the DNO regarding the degree of “firmness” provided through their connection to the distribution system?
- How, if at all, does the need for a prescriptive planning standard change as consumers receive smart meters, and so could (in theory) receive signals through tariffs regarding the availability of network capacity in real time? For instance, real time DUoS charges could signal scarcity of network capacity when it arises, and encourage consumers to curtail load.

**Response:**

**Additional Comments:**

**Response Status (please indicate):**

- Response to remain anonymous (default).
- Share the response but without reference to company or project.
- Share the response with other respondents willing to share their information

**Question 2.6:**

Should the planning standard prescribe the (minimum) level of network security for smaller sizes of group demand (e.g. for class supply A-C) or should other regulatory incentives (such as IIS or other additional incentive mechanisms) be used that could provide a higher (incentivised) level of network security?

**Response:**



<b>Additional Comments:</b>
<b>Response Status (please indicate):</b>
<input checked="" type="checkbox"/> Response to remain anonymous (default).
<input type="checkbox"/> Share the response but without reference to company or project.
<input type="checkbox"/> Share the response with other respondents willing to share their information

<b>Question 2.7:</b>
How do you understand how customers value security? In planning your network and conducting cost-benefit analysis, what economic value do you place on improvements in reliability, i.e. the reduced risk of interruptions? For example, do you specify consumer damage functions, or use more simplistic representations of customer damage, such as the IIS incentive rates? How has the value placed on network security by customers been changing in recent years? How do you expect it to change in the future, e.g. due to developments such as the increased reliance of the heat and transport sectors on the electricity system?"
<b>Response:</b>
<b>Additional Comments:</b>
<b>Response Status (please indicate):</b>
<input checked="" type="checkbox"/> Response to remain anonymous (default).
<input type="checkbox"/> Share the response but without reference to company or project.
<input type="checkbox"/> Share the response with other respondents willing to share their information

<b>Question 2.8:</b>
Do you see any impact from the deployment of smart meters on network security planning standards?
<b>Response:</b>
<b>Additional Comments:</b>
<b>Response Status (please indicate):</b>

- Response to remain anonymous (default).
- Share the response but without reference to company or project.
- Share the response with other respondents willing to share their information

**Question 2.9:**

What changes to the current RIIO framework, in your view, would better promote efficient levels of investment to promote security of supply?

**Response:**

**Additional Comments:**

**Response Status (please indicate):**

- Response to remain anonymous (default).
- Share the response but without reference to company or project.
- Share the response with other respondents willing to share their information

**Question 2.10:**

What impact (if any) does the IIS have on your system design?  
 What interaction is there between the planning standard and requirements specified by IIS?

**Response:**

**Additional Comments:**

**Response Status (please indicate):**

- Response to remain anonymous (default).
- Share the response but without reference to company or project.
- Share the response with other respondents willing to share their information

**Question 2.11:**

In reforming P2/6, do you consider there is a need for consistency with the NETS SQSS that we should consider and if so, to what extent?  
 What other interactions do you see between P2/6 and other regulatory and industry codes?

Are there any specific conditions that should be included?

**Response:**

**Additional Comments:**

**Response Status (please indicate):**

- Response to remain anonymous (default).
- Share the response but without reference to company or project.
- Share the response with other respondents willing to share their information

**Question 2.12:**

Should the planning standard explicitly consider extreme events?  
If so, how should the standard cater for High Impact, Low Probability (HILP) conditions such as extreme weather or ICT failures?

**Response:**

**Additional Comments:**

**Response Status (please indicate):**

- Response to remain anonymous (default).
- Share the response but without reference to company or project.
- Share the response with other respondents willing to share their information

## 5 SECTION 3: REAL TIME NETWORK OPERATION AND SECURITY OF SUPPLY

In this section of the questionnaire, we seek views and feedback regarding the changes in real time network operation and control that could be facilitated through new software applications and supporting ICT infrastructures that will be available to facilitate the transition to a "smart grid" paradigm, with specific focus on the impact on security of supply.

<b>Question 3.1:</b>
What are your experiences of the impact on security of supply as a result of changes in real time network operation and control in support of the deployment of "smart" devices on the network?
<b>Response:</b>
<b>Additional Comments:</b>
<b>Response Status (please indicate):</b>
<input checked="" type="checkbox"/> Response to remain anonymous (default).
<input type="checkbox"/> Share the response but without reference to company or project.
<input type="checkbox"/> Share the response with other respondents willing to share their information

<b>Question 3.2:</b>
To support the move towards a "smarter" network, what Information and Communications Technology (ICT) infrastructure have you developed, or plan to deploy, on the network to have an (positive) impact on the security of supply?
<b>Response:</b>
<b>Additional Comments:</b>
<b>Response Status (please indicate):</b>
<input checked="" type="checkbox"/> Response to remain anonymous (default).
<input type="checkbox"/> Share the response but without reference to company or project.
<input type="checkbox"/> Share the response with other respondents willing to share their information



**Question 3.3:**

What experience have you gained and (any) lessons learnt from real-time system control (including supporting ICT requirements) relating to system security, from LCNF projects and/or any other associated pilot studies or trials?

Please provide any relevant example project references that we may investigate further.

**Response:**

**Additional Comments:**

**Response Status (please indicate):**

- Response to remain anonymous (default).
- Share the response but without reference to company or project.
- Share the response with other respondents willing to share their information

## 6 SECTION 4: ADDITIONAL QUESTIONS AND POINTS FOR CONSIDERATION

Are there any additional points that you believe should be considered during the analysis phase of the project or included in the wider review?

These may include:

- Transparency and practicality of the future standard.
- Acceptability and application.
- Others related issues.

Please complete any additional tables as required.

<b>Question 4.X:</b>
<b>Response:</b>
<b>Additional Comments:</b>
<b>Response Status (please indicate):</b>
<input checked="" type="checkbox"/> Response to remain anonymous (default).
<input type="checkbox"/> Share the response but without reference to company or project.
<input type="checkbox"/> Share the response with other respondents willing to share their information

## 7 CONTACTS

Name	Company	Address	Email	Phone details
Colin MacKenzie	DNV GL	Palace House 3 Cathedral Street London SE1 9DE	<a href="mailto:colin.mackenzie@dnvgl.com">colin.mackenzie@dnvgl.com</a>	Mobile: 07557741627
Alan Birch	DNV GL	Palace House 3 Cathedral Street London SE1 9DE	<a href="mailto:Alan.birch@dnvgl.com">Alan.birch@dnvgl.com</a>	Mobile: 07557741624
Goran Strbac	Imperial Consultants	Imperial College London SW7 2AZ	<a href="mailto:g.strbac@imperial.ac.uk">g.strbac@imperial.ac.uk</a>	Mobile: 0797365 8976
Richard Druce	NERA	Marble Arch House 66 Seymour Street London W1H 5BT	<a href="mailto:richard.druce@nera.com">richard.druce@nera.com</a>	Mobile: 07962076267

## APPENDIX B LIST OF STAKEHOLDER ORGANISATIONS INVITED TO RESPOND TO THE QUESTIONNAIRE.

Stakeholders that make use of the ER P2/6 on a regular basis

Company Name
Electricity North West Limited
Northern PowerGrid
Scottish and Southern Energy - Power distribution
Scottish Power Energy Networks
Western Power Distribution
Uk Power Network
Northern Ireland Electricity
National Grid
Ofgem
DECC

Wider group of interested parties and industry participants

Company
GTC-UK
Energetics Electricity Limited
ESP Electricity Limited
Transmission Capital Partners
Power Con
GTC-UK
RES
SmartGrid GB
RenewablesUK
Scottish Renewables
Renewable Energy Association
British Hydro Power Association
British Photovoltaic Association
Solar Trade Association
Energy UK
Energy Storage Network
Renewable energy systems Ltd (RES)
UK Demand Response Association
Association of Decentralised Energy
Energy Innovation Centre



Primrosesolar
Smart Energy Demand Coalition
AMPS



## About DNV GL

Driven by our purpose of safeguarding life, property and the environment, DNV GL enables organizations to advance the safety and sustainability of their business. We provide classification and technical assurance along with software and independent expert advisory services to the maritime, oil and gas, and energy industries. We also provide certification services to customers across a wide range of industries. Operating in more than 100 countries, our 16,000 professionals are dedicated to helping our customers make the world safer, smarter and greener.