

## Alternative approaches to breach, under an access sharing arrangement

The present breach provisions covering bilateral connection agreements and the CUSC relating to Use of System issues are contained in 5.4.1 to 5.4.3 of the CUSC. Essentially if a generator breaches its total access holding then National Grid can issue a notice requiring the generator to confirm that it will not repeat the breach. **The generator and National Grid are required to discuss in good faith how best to avoid a future breach.** If ~~the~~ generator does repeat the breach then the SO may de-energise the equipment of the relevant User.

At the Transmission Access Working Group 1 meeting, we discussed whether these breach provisions were appropriate for the sharing of access as envisaged under CAP163 ('Entry Capacity Sharing'), particularly when the individual party which caused an overrun on the sharing arrangement could not be identified. The following sets out two alternative approaches that could be used in such circumstances. It is expected that a formal overrun product would be the most appropriate solution, but the options below seek to provide a credible alternative, should CAP162 ('Entry Overrun') not be approved.

We assume that the donor and recipient<sup>1</sup> have a bilateral sharing agreement with each other which determines how they share the capacity with each other. It is not for the SO to worry how the total capacity is shared between the two parties, just to ensure that the aggregate level is not breached. In order to do this it will be necessary for the donor and recipient to inform the SO that they have a sharing agreement between power station X (the donor site) and power station Y (the recipient site). With this information the SO will be able to calculate the aggregate level of access (long and short term, as appropriate) held by these two sharing sites.

There are three main scenarios which can lead to the breach:

- A) The donor breaches its agreed level under the sharing agreement, but the recipient does not.
- B) The recipient breaches its agreed level under the sharing agreement, but the donor does not.
- C) Both donor and recipient breach their sharing agreement.

Ideally, the arrangements would target the donor under scenario A, the recipient under scenario B and both of them under scenario C. Under an arrangement where the parties have notified centrally to the SO the two quantities of access to be shared at the respective power stations (eg. power station X will share 100MW with power station Y, so the access of X will reduce by 100MW and Y will increase by 100MW) this would be possible to do directly.

---

<sup>1</sup> We assume, for simplicity, a single recipient: the possibility of multiple recipients sharing a single donor's access should also be considered.

However, when the aggregate position is only known then any sanctions can only be applied to the sharing parties collectively, thereby relying on them to make appropriate arrangements to cover their individual positions through their bilateral sharing agreement. Thus, in our example above, the aggregate level of access is 100MW. If the SO sees, in aggregate, the two power stations have done 110MW the SO does not know which of them has breached, just that in aggregate they have both breached.

~~The two options for alternative approaches relating to breach of sharing arrangements are as follows are outlined in this paper. One option extends the existing It is assumed that they would replace the provisions for issuing a notice and de-energising contained in 5.4 as discussed above to operate with sharing arrangements. The other option introduces alternative arrangements which it is envisaged would replace the arrangements in 5.4 for breaches of both individual holdings of access rights as well as breaches of sharing arrangements. However, there may be the requirement to maintain the threat of de-energising for persistent offenders.~~

~~It is also anticipated that these provisions would be applied to all breaches of access rights. That is they wouldn't just apply to circumstances where access rights were being shared. This would allow consistent arrangements to be applied against capacity rights breaches in all scenarios. Therefore, for example, a generator breaching its TEC would be treated the same regardless of whether or not this had been shared with another party.~~

## **1. Scale back arrangement in proportion to size of total breach**

This option provides for the aggregate total access rights under the sharing arrangement to be scaled down in the event of a breach. For instance, if the total amount of capacity covered by the arrangement is 500MW and the two power stations run to a total of 520MW then the effective capacity of the arrangement from then on could be scaled down to  $500\text{MW} * 500/520$  or about 481MW. Alternatively, the amount of over-generation could be subtracted from the shared access rights so that in the above example the rights would be scaled to  $500\text{MW} - (520-500)\text{MW} = 480\text{MW}$ . An identical approach could be applied to access rights breaches by single generators.

This would have two effects. Firstly, it would act as an incentive against breach as the sharing arrangement would be reduced in value. Secondly, if a similar sized breach were to occur again, the level of capacity used would be no higher than the level of the original sharing arrangement.

The parties would be able to agree between themselves what this meant for their individual capacities under the bi-lateral sharing agreement. This would be a matter for them, but presumably an equitable solution would be for the offending party to take on the full level of the reduction rather than it to be shared between both the offending and innocent parties. Thus, in our example above, the offending party would see its access, under the sharing

agreement, decline by 19MW or 20MW depending on the method of scale back.

This flexible arrangement wouldn't sterilise all of the capacity in the arrangement or all of a single generator's access rights, but would still act as a deterrent against breaching access rights, therefore providing some protection to other Users.

There may be a requirement for some form of backstop arrangement to avoid persistent breaches. This mechanism could work each time a breach occurred which would potentially scale down the level of access reasonably quickly. For instance, if the parties in the example generated at 500MW following the scaling of their rights to 480MW, their rights would be scaled to 460MW. If they continued to generate at 500MW they would be scaled to 420MW, 340MW, 180MW and then zero. Once a generator's capacity had been reduced to zero, the generator/s could be de-energised as provided for under the present CUSC arrangements.

It has been considered by the group whether or not there should be a threshold within which small fluctuations would be allowed such as 2% of the rights held. However, this has **initially** been discounted as it is believed that this would provide an incentive for generators to hold access rights at 98% of those they anticipated they actually required.

The timescales for the process by which these arrangements are invoked would have to be determined. The present breach provisions **give- have no set timescales for** National Grid **28-days** to notify the breaching party. **However, after such a notice is issued the relevant party-which it** has 5 working days to confirm that it will not repeat the breach. This process **potentially** needs to work **far** more quickly than this **and at least there needs to be greater certainty as to the timescales**. Therefore, it is expected that National Grid would be able to issue a notice in a matter of hours, or one **of-or** two days at the latest. Following this, there should be a query period to allow the party or parties concerned to respond with any alternative data. Again, this should not be a long period with one of two days being allowed at a maximum. Ultimately, we would expect that the matter could be referred to the Authority if National Grid and the party concerned cannot agree that the breach has taken place or on the size of the breach.

Another matter for consideration is how long the reduction in rights is **affective effective** for. This could be a number of days, weeks or at the extreme months **[any views anyone?]**. Additionally, termination or expiration of a sharing agreement should not result in the rights being fully reinstated. In this event the reduction should be maintained on the same basis as if the agreement had not been terminated or had not expired.

## **2. Use a post event dispute with present breach provisions**

Another option would be to use a post event dispute mechanism to identify the party that caused the breach of the shared TEC arrangement. This would allow the present provisions of 5.4 to be applied to that party. A number of issues considered under the option 1 above would not be required under this option, as they would follow the existing provisions of the CUSC.

The timescales for raising the notification of breach may need to be reconsidered. As with option 1 above, the ~~28 days presently~~time provided for ~~this at present~~ may be seen as too ~~vague and potentially too long to effectively deal with access rights breaches~~. However, this option also could lead to de-energisation of the party far more quickly than option 1. Therefore, the timescales should be such that sufficient time is given to identifying the party responsible for the breach and for the consideration of any query or appeal by the parties ~~[any views all?]~~.

An issue to consider is what to do if no party is willing to be identified as causing the breach. The solution ~~could~~ be to implement the provisions of 5.4 on both parties. This would potentially provide an incentive for the innocent party to provide evidence of ~~its~~ innocence and of the other party's role in causing the breach.

Another issue to be addressed is what is meant by a material adverse effect which is required to occur before de-energisation is allowed under the CUSC? The only definition of materiality in the CUSC at present is £10,000 and this is in the context of changes in works associated with providing a connection of use of the system. A better definition ~~would~~may relate in these circumstances to the size of over run by the generator ~~[any ideas?]~~.

## Comparison of options 1 and 2

Option 2 would be the simpler of the two options to implement. Most of the issues covered under option 1 above would follow the existing provisions in the CUSC. However, option 2 is ~~also potentially~~ a more extreme sanction than option 1. ~~In The sanction in option 2 there is a "one strike and you're out approach" which results in~~ de-energisation of the generator or generators concerned, which may be seen as too heavy handed to deal with relatively small breaches of rights. ~~Option 1 may be seen as more proportionate, acting as a deterrent without removing all of the party's rights. One mitigating feature is that, as an extension of the existing breach provisions, Option 2 only requires that breaches which have a "material adverse effect" are addressed. If this is seen as a desirable feature and if a definition of what is material can be derived, it could be introduced for both Options 1 and 2.~~

~~#Option 2 may also be viewed as too cumbersome if the number of breaches increases as a result of parties sharing rights. Option 1 may be seen as more proportionate, acting as a deterrent without removing all of the party's rights.~~

Therefore, the choice of which option to choose **also** comes down to what you believe the future pattern of breaches might be as well as your view as to the success of the overrun product defined in CP162.

A summary of the main aspects of the two options are summarised as follows

	Option 1: Scaled Rights	Option 2: Extend Existing Breach Provisions
Ease of implementation	X	✓
Proportionality of response	✓	X
Ability to be backed off in bilateral sharing agreement	✓	X
Protection to other users	✓	✓✓
Ability to deal with larger numbers of breaches	✓	X

### **Next steps**

The working group 1 members are requested to decide the following issues:

1. Which option to progress.
2. What should be the definition of material? A MW figure could be set, noting that this would potentially allow smaller generation plant to overrun by a significant proportion. Alternatively, a percentage overrun threshold of say 2% could be reconsidered by the group? Larger generators could have a higher individual effect with this option. A combined approach of the above two could be employed.
3. For how long should rights be scaled in Option 1? There needs to be a balance between it being long enough a period to be a deterrent, but not so long that it is overly penal. What would the group suggest: two weeks; a month?
- 4.4. What should the timescales be for processing the breach? For option 1 there is the time National Grid has to notify the party or parties of the breach, the time to raise any query, the time to address that query and then the time to scale back the rights.

For option 2 there is the time National Grid has to notify the party or parties of the breach, the time to raise any query, the time to address that query and the time for the party or parties to undertake not to repeat the breach. Then, if there is a repeat of the breach, there are

similar timescales required to run up to de-energisation of the party or parties concerned.

~~10th July, 2008~~ 14 August, 2008

## Appendix 1 – Current Breach Provisions

### 5.4.1 Site Specific Breach by the User

If a **User** shall be in breach of any of the provisions of the relevant **Bilateral Agreement**, or the provision of the **CUSC** in relation to that particular connection to and/or use of the **GB Transmission System**, or (other than in relation to a **Supplier**, a **Small Power Station Trading Party**, an **Interconnector User** or an **Interconnector Error Administrator**) of the provisions of the **CUSC** enforcing the provisions of the **Grid Code** (but subject always to Paragraphs 6.3.3 and 6.3.4), and such breach causes or can reasonably be expected to cause a material adverse effect on the business or condition of **The Company** or other **Users** or the **GB Transmission System** or any **User Systems** then **The Company** may:-

(a) where the breach is capable of remedy, give written notice to the **User** specifying in reasonable detail the nature of the breach and requiring the **User** within 28 days after receipt of such notice, or within any longer period agreed between **The Company** and the **User** to remedy the breach, the agreement of **The Company** not to be unreasonably withheld or delayed; or

(b) where the breach is incapable of remedy, give written notice to the **User** specifying in reasonable detail the nature of the breach and the reasons why the breach is incapable of remedy and requiring the **User** within 5 **Business Days** after receipt of such notice to undertake to **The Company** not to repeat the breach.

### 5.4.2 Grid Code Procedures - Future Compliance

Whenever **The Company** serves a notice on a **User** pursuant to Paragraph 5.4.1, **The Company** and the **User** shall discuss in good faith and without delay the nature of the breach and each shall use all appropriate procedures available to it under the **Grid Code** (including testing rights and the procedures set out in **OC5** (Testing and Monitoring)) in an attempt to establish as quickly as reasonably practicable a mutually acceptable way of ensuring future compliance by the **User** with the relevant provision of the **Grid Code**.

### 5.4.3 Site Specific Deenergisation

(a) If:

- (i) a **User** fails to comply with any valid notice served on it by **The Company** in accordance with Paragraph 5.4.1(a) or is in breach of any undertaking given in accordance with Paragraph 5.4.1(b) and such breach causes or can be reasonably expected to cause a material adverse effect on the business or condition of **The Company** or other **Users** or the **GB Transmission System** or any **User System**; or

- (ii) five **Business Days** have elapsed since the date of any valid notice served on the **User** in accordance with Paragraph 5.4.1(b) and no undertaking is given by the **User** in accordance with Paragraph 5.4.1(b);

**The Company** may:

- (iii) provided **The Company** has first complied with **OC5** Monitoring and Testing if appropriate **Deenergise** the **User's Equipment**; or
- (iv) provided **The Company** has first complied with **OC5** Monitoring and Testing if appropriate request the owner/operator of the **Distribution System** to which the **User's Equipment** or equipment for which the **User** is responsible (as defined in Section K of the **Balancing and Settlement Code**) is or to which the **User's Customers** are connected to **Deenergise** the **User's Equipment** or equipment for which the **User** is responsible (as defined in Section K of the **Balancing and Settlement Code**) at the relevant site of connection or such **User's Customers** (as the case may be); or
- (v) in the case of an **Interconnector User** or **Interconnector Error Administrator** request the relevant **Interconnector Owner** to cease or procure the cessation of the transport of power by or on behalf of that **User** across the **Interconnector**,

upon the expiry of at least 48 hours prior written notice to the **User**, provided that at the time of expiry of such notice the breach concerned remains unremedied and that neither party has referred the matter to the **Dispute Resolution Procedure**. In such event **The Company** may:

- (aa) **Deenergise** the **User's Equipment**, or
- (bb) request the owner of the **Distribution System** to which the **User's Equipment** or equipment for which the **User** is responsible (as defined in Section K of the **Balancing and Settlement Code**) is or to which the **User's Customers** are connected to **Deenergise** the **User's Equipment** or equipment for which the **User** is responsible (as defined in Section K of the **Balancing and Settlement Code**) at the relevant site of connection or the **User's Customers** (as the case may be), or
- (cc) in the case of an **Interconnector User** or **Interconnector Error Administrator** request the relevant **Interconnector Owner** to cease or to procure the cessation of the transfer of power by or on behalf of that **User** across the **Interconnector**, forthwith following completion of the **Dispute Resolution Procedure** and final determination of the dispute in **The Company's** favour, subject to **The Company** having given, in the case of **Deenergisation** of an **Embedded Small Power Station**, the relevant **User** not less than

24 hours prior written notice and at the expiry of such notice the breach concerned remaining unremedied.

(b) If the **User** fails to comply with the **Grid Code** (but subject always to Paragraphs 6.3.3 and 6.3.4 of the **CUSC**) and the **Authority** makes a final order or a confirmed provisional order as set out in sections 25 and 26 of the **Act** against the **User** in respect of such non-compliance which order the **User** breaches **The Company** may in respect of the relevant **Connection Site(s)** or site(s) of connection:

- (i) **Deenergise the User's Equipment**, or
- (ii) request the owner of the **Distribution System** to which the **User's Equipment** or equipment for which the **User** is responsible (as defined in Section K of the **Balancing and Settlement Code**) is connected to **Deenergise the User's Equipment** or equipment for which the **User** is responsible (as defined in Section K of the **Balancing and Settlement Code**),

upon the expiry of at least 48 hours prior written notice to the **User** provided that at the time of expiry of the notice the **User** continues to fail to comply with the order.