Additional points in response to question 3 of the CMP432 Work Group Consultation

Uniper would like to make the following additional points in response to question 3 as an attachment, as they would be difficult to include and read in the proforma:

1. The current methodology correctly mixes forward looking with average historic costs

This is deliberate. It needs to be able to:

- Provide locational signals based on incremental usage of the network.
- Balance this with stability, predictability and fairness.
- Promote efficient use of the existing network as well as new network investments.

The CUSC is clear is saying that incremental costs are calculated using MWkm. Paragraph of 14.15.4 of the CUSC states (our emphasis):

"*The DCLF ICRP transport model calculates the marginal costs of investment in the transmission system which would be required as a consequence of an increase in demand or generation at each connection point or node on the transmission system, based on a study of peak demand conditions using both Peak Security and Year-Round generation backgrounds on the transmission system.* ***One measure of the investment costs is in terms of MWkm. This is the concept that ICRP uses to calculate marginal costs of investment***."

The MWkms need to be multiplied by a cost per MWkm. This is provided through a combination of the Expansion Constant, the Expansion Factors and the Locational Security Factor. These are calculated on a more average basis, not least to prevent volatile changes in value year on year which would undermine charge predictability.

This second purpose of balancing predictability and stability is a well established principle in TNUoS charging. Indeed, in the context of the Locational Security Factor, this was recognised by the Authority in March 2005 in its decision on NGC's proposed GB electricity transmission use of system charging methodology (our emphasis).

"*In principle the Authority considers that charges which are* ***reflective of costs*** *(including in taking account of network security),* ***are fair and reasonable, have an appropriate degree of transparency and stability, and which are applied in a non-discriminatory manner****, would be expected to be proportionate and consistent with the relevant European law, including the requirements of the IMED and the Renewables Directive.*"[1]

It is correct that security should be reflected in the cost of the network as the provision of security requires more network to be built than would otherwise be the case. Again, at the time

[1] NGC's proposed GB electricity transmission use of system charging methodology The Authority's decisions – March 2005 https://www.ofgem.gov.uk/sites/default/files/docs/2005/03/10033-8005_0.pdf

when NGC's methodology was being decided upon by the Authority this was recognised, this time in December 2004 (our emphasis):

"*2.11 Transmission networks are developed to comply with relevant engineering planning standards. These standards require that sufficient capacity is built to accommodate flows across the network when circuits are, as a result of faults or planned maintenance work, not available. The cost of providing additional capacity is therefore driven by the cost of providing a network secured against such faults and outages.*

2.12 The DCLF used by NGC assumes that all circuits are available. It is therefore an 'unsecured' model. NGC calculate a security factor as an estimate of the average difference (in terms of additional electrical flows) between the unsecured DCLF and a secured load flow model. NGC calculate the security factor to be equal to 1.8. ***This could be interpreted as saying that approximately 80% more capacity needs to be provided as contingency against network faults than would be required if faults and outages did not occur.****"*[2]

CMP432 would remove all reflection of this additional network cost reality.

2. The stylised models used in support of CMP432 only show implied incremental security factors of one in certain circumstances

As we mention elsewhere, Uniper does not agree with the rationale for CMP432 that the Locational Security Factor should be fully forward looking. We support the existing principle of a LSF based on current security of the network. This is consistent with the current way that the model and methodology works and balances an incremental approach which is facilitated by the calculation of incremental MWkms, with a more average approach when calculating the average cost of network assets, which promotes predictability, fairness and also provides incentives for efficient use and reuse of existing networks assets.

Nevertheless, we also feel that it is important to address the assertion that the transmission network will only be reinforced in future to provide transfer capacity and not to provide additional security. The arguments that have been made to this effect in the workgroups and consultation document focus on looking at individual network investments, either in a stylised way or by looking at actual single circuit investments.

The first thing we would note is that the stylised examples only appear to work to demonstrate an implied incremental LSF of 1 when the new asset that is built is a single circuit which is smaller in size than those that were in place before it (and so is not secured against following investment). This can be illustrated by the following examples:

[2] NGC's proposed GB electricity transmission charging methodologies The Authority's decisions - December 2004 https://www.ofgem.gov.uk/sites/default/files/docs/2004/12/9096-27504.pdf

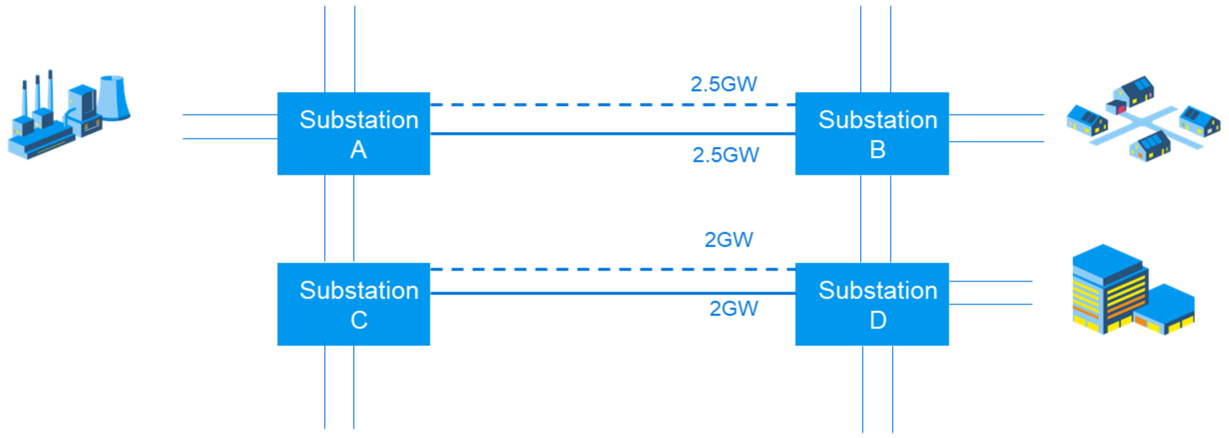

Figure 1: Stylised example pre investment

Figure 1 above shows a stylised example similar to that presented in the workgroups. The arrangement provides 9GW of thermal capacity, but as it needs to be secured against the loss of two largest routes (the dotted 2.5GW and 2GW circuits shown on the diagram) the secured flow that can be accommodated is 4.5GW (2.5GW + 2GW remaining solid line circuits).

Figure 2 is similar to the example presented to the workgroup, where an additional 1GW of thermal capacity is provided through a single additional circuit between the substations C and D. In this example, the thermal capacity is increased by the additional 1GW to 10GW. As the new circuit is not one of those the loss of which would need to be secured against, then the secured flow is also increased by 1GW to 5.5GW (2.5GW + 2GW + 1GW). Therefore, it's implied incremental security factor is 1.

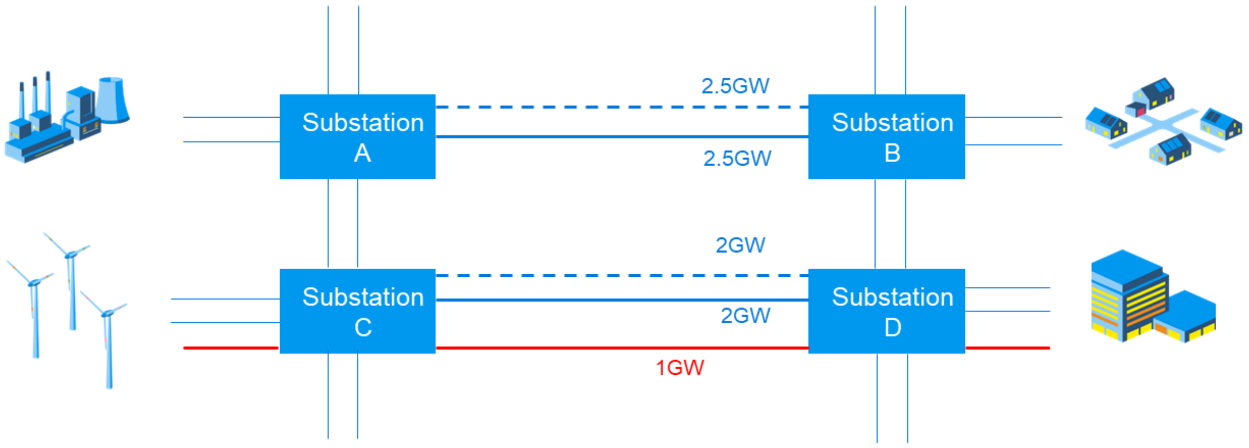

Figure 2: Add 1GW of capacity through a new single circuit (new circuit is smallest capacity so not secured against)

Figure 3 shows a similar example where an additional thermal capacity of 2.5 GW is provided, in a similar manner to that shown in figure 2. As the circuit is relatively large compared with those there previously, it is one of the lost circuits that needs to be secured against. In this instance, the thermal capacity increases by 2.5GW to 11.5GW, but the secured flow increases by 2GW to

6.5GW (2.5GW + 2GW + 2GW). This implies an incremental security factor of 1.25 (2.5GW increase in thermal capacity divided by 2GW increase in secure flow).

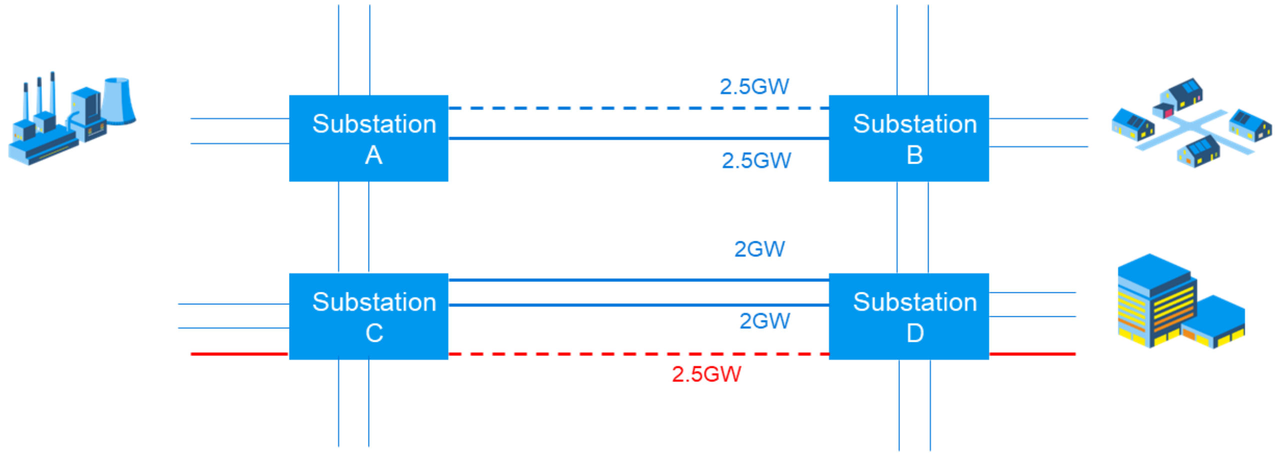

Figure 3: Add 2.5GW of capacity through a new single circuit (new circuit is secured against)

Figure 4: shows an example where the thermal capacity of the route is increased by 2GW, by reinforcing the existing circuits by 1GW each. In this example, the thermal capacity is increased to 11GW (9GW + 2GW). However, the loss of one of the new 3GW circuits has to be secured against. In this instance, secured flow increased by 1GW to 5.5GW (2.5GW + 3GW). Therefore, the implied incremental security factor is 2 (2GW increase in thermal capacity divided by 1GW increase in secure flow).

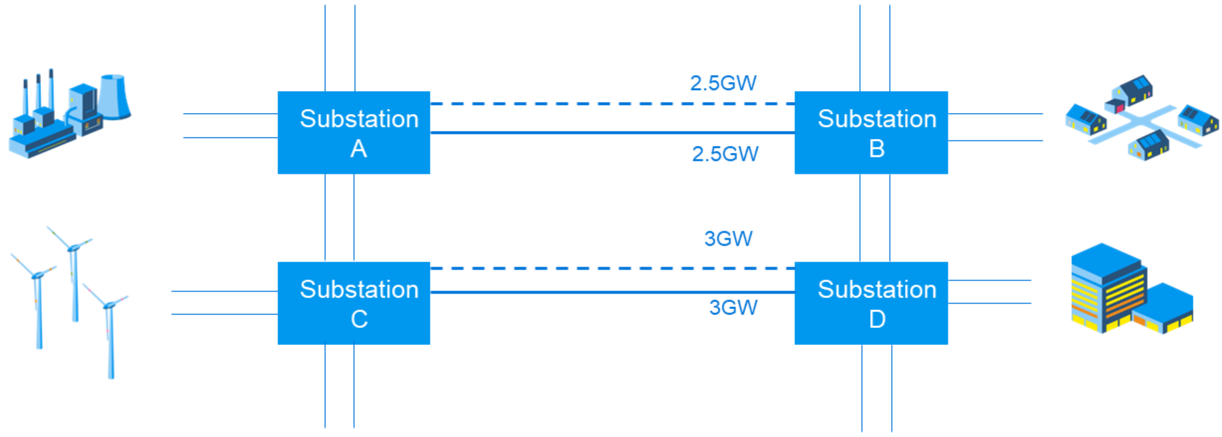

Figure 4: Add 2GW of capacity through upgrading existing circuits

Therefore, even using these stylised examples it is clear that different scenarios can imply an incremental LSF of between 1 and 2.

3. It is not appropriate to calculate incremental security for new single circuits

However, we do not believe that it is actually appropriate to analyse single investments in the network in this manner. Network security is provided by the creation of a meshed network of multiple routes, which provide alternative paths for power to flow should one part of the network fail. Measuring security in a purely forward looking manner by analysing the impact of individual circuits is an inappropriate way to measure security. Individual circuits cannot provide security on their own, they can only do so in combination with others.

Therefore, it would be more accurate to analyse how the network is planned to be built over the coming years as a whole. NESO's planning documents given an insight into this. Its Holistic Network Design summary report[3] shows HND recommended network requirements and those that have been previously recommended. This is reproduced in Figure 5 below. It shows that the expected future network is required to become significantly more meshed, particularly in respect of north to south flows within the country, mainly provided by new offshore network assets, but also through reinforcement of existing routes onshore. A similar position is shown in NESO's report on the position beyond 2030[4]

Specific information on the amount of security provided by investments does not appear to be available. However, it does appear to be the case that additional security will be provided by increasing the meshed nature of the network, particularly offshore. There is also a significant amount of upgrading of existing lines.

---

[3] Pathway to 2030 - July 2022 https://www.neso.energy/document/262676/download
[4] Beyond 2030 – March 2024 https://www.neso.energy/document/315516/download

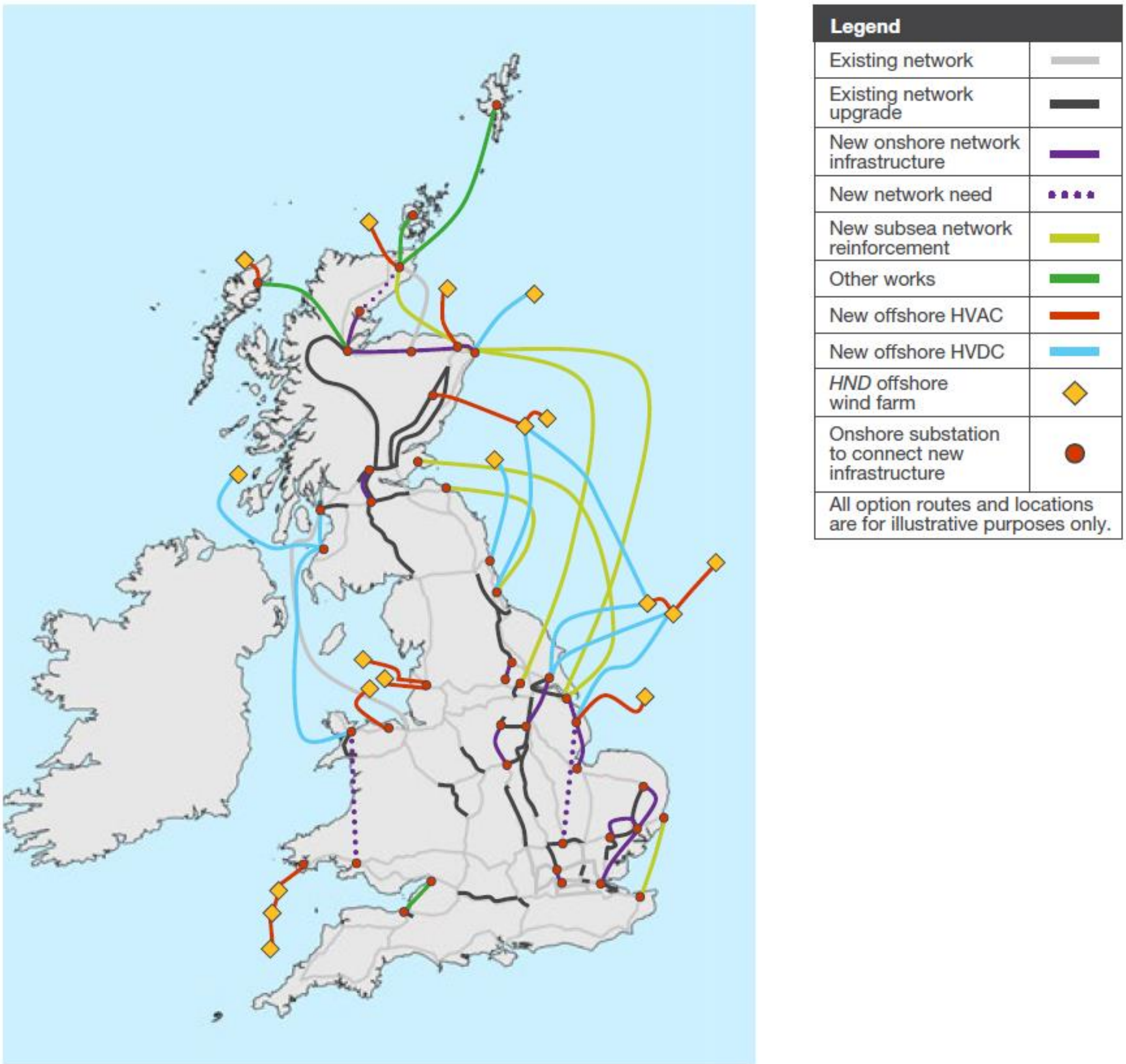

Figure 5: Diagram of HND and previously recommended network requirements (Source: NESO - Figure 3 of the Pathway to 2030 July 2022)

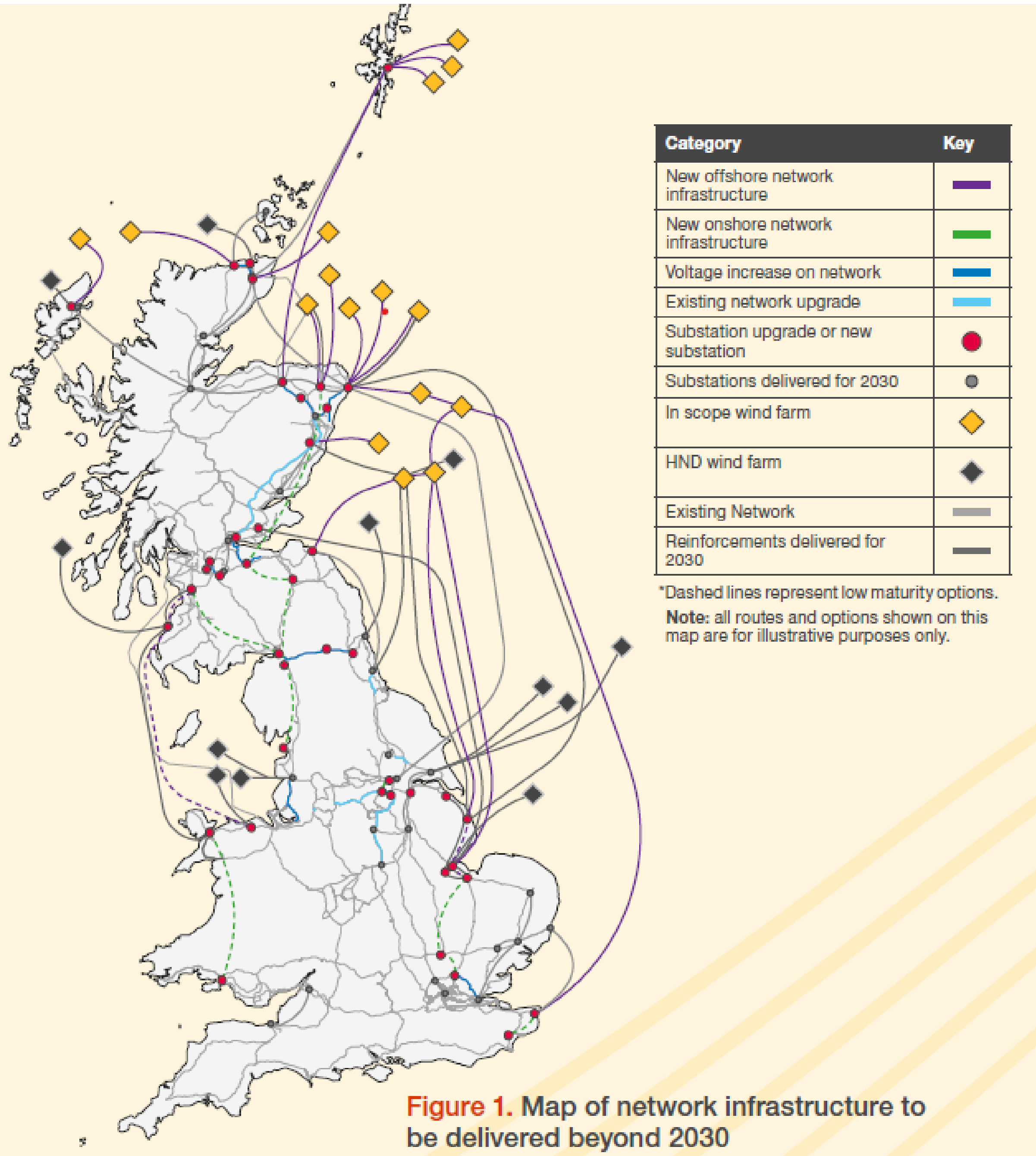

Figure 6: Taken from NESO's Beyond 2030 – March 2024

We considered whether it is possible to estimate the amount of additional network that has been built to provide existing secured flow capability in the current meshed system by looking at a key boundary. Figure 7 below shows a diagram from NESO's 2018 Electricity Ten Year

Statement (ETYS)[5] showing the circuits that cross the B6 boundary. It has been annotated to show the capacity in MVA for the onshore network and MW for the offshore HVDC link. Onshore network asset capacities have been taken from Appendix B of the ETYS and the HVDC link from the information on the B6 Boundary in the main section of the ETYS. Assuming a 1:1 relationship between MVA and MW, it shows that the full thermal capacity of the assets crossing the boundary is 12.2GW whereas the stated boundary transfer capacity is 5.7GW. If this were to be used to imply a LSF for that boundary it would be 2.14. Prior to the HVDC link being installed the transfer capacity was 3.5GW supported by installed assets of 10GW. This would imply a prior LSF of 2.86.

We actually believe that such an analysis is likely to be over simplistic and does not take into account other factors from other parts of the network which will influence the actual boundary capability. However, it is another way of looking at the analysis that has been carried out in support of CMP432 to estimate the incremental security provided by the Western HVDC link. Looking at a single asset and trying to estimate its sole incremental contribution to security doesn't make sense, as single circuits cannot provide security in isolation from other circuits. It is the total interaction of the wider network assets as a whole that provides this and which is important. For instance, we note that since the 2019 ETYS, the capability of the network over the B6 boundary has changed several times due to changes in conditions on the network, rather than investment in new assets.

This makes sense when you consider that wider factors drive the level of security of the system in a widely meshed network. It would suggest another reason for adopting a system wide average figure for security. The level of redundancy appears difficult to calculate for smaller discrete elements of the network because of these interactions, even when all of the circuits that contribute to a boundary are considered.

[5] 2018 Electricity Ten Year Statement https://www.neso.energy/document/133836/download

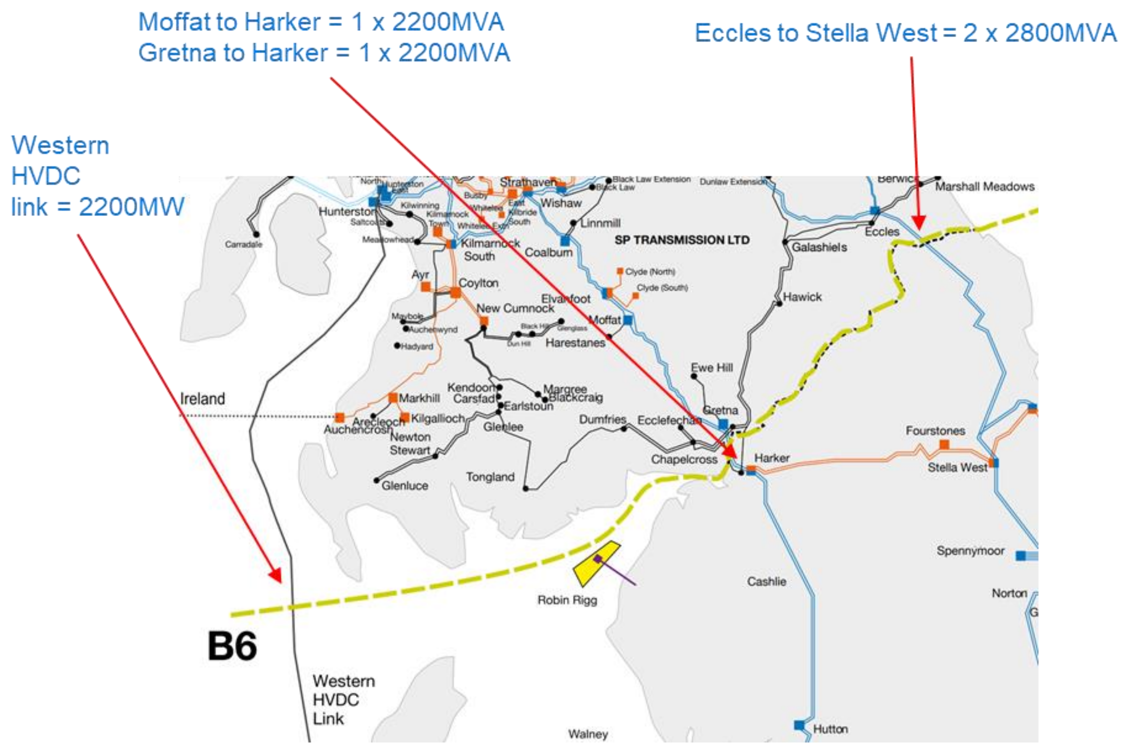

Figure 7: Circuits that cross the B6 boundary (source Electricity Ten Year Statement 2018)

4. Treatment of HVDC assets in the model

CMP432 is predicated on an assumption that future network reinforcements will tend to look like the Western HVDC link and that only the incremental effect of adding such assets should be considered in the calculation of the security factor and not the effect of existing assets. Whilst we disagree with this argument, if its logic is followed then the model should not seek to use existing assets when calculating MWkms either.

However, the current model does just that and deliberately so. A very specific example of this is in the calculation of the percentage use of HVDC circuits. The Western HVDC link was built to provide additional transfer capacity from north to south in the network as the current network was deemed insufficient to accommodate increased north-south flows required for additional generation connecting in the north of GB. Therefore, it would be totally reasonable to assume that the link would provide the vast majority, if not the full amount, of incremental MWkm for new plant connecting north of it. However, the current methodology presently assumes that the link is only used proportionately to the rest of the network. Therefore, in the most recent transport model, the HVDC link provides 8% of the north-south flow with the rest of the flow being accommodate on existing onshore assets. For the year round background, the figure increases to around 26% (averaging the effects over the B6 and B7a boundaries that are considered for this purpose in the model).

If the flows were treated on the purely incremental basis and therefore allocated to the HVDC assets, then of course the MWkms associated with those boundary flows would be considerably higher. An additional 92% to 74% of the costs of these flows would be costed using HVDC Expansion Factors.

We believe that the model should be constructed on a consistent basis. As it currently utilises a mixture of new and existing assets by design, any move away from that principle should be carried out consistently across all elements of the model and methodology to ensure that all elements interact appropriately. This would require a wider holistic approach to change rather than a piecemeal change to one aspect which would distort signals and undermine competition.