Public

Workgroup Consultation Response Proforma

CMP432: Improve "Locational Onshore Security Factor" for TNUoS Wider Tariffs

Industry parties are invited to respond to this consultation expressing their views and supplying the rationale for those views, particularly in respect of any specific questions detailed below.

Please send your responses to cusc.team@nationalenergyso.com by **5pm** on 07 March 2025. Please note that any responses received after the deadline or sent to a different email address may not receive due consideration.

If you have any queries on the content of this consultation, please contact: cusc.team@nationalenergyso.com

Respondent details	Please enter your details	
Respondent name:	John Tindal	
Company name:	SSE	
Email address:	John.tindal@sse.com	
Phone number:	Click or tap here to enter text.	
Which best describes your organisation?	☐Consumer body ☐Demand ☐Distribution Network Operator ☒Generator ☐Industry body ☐Interconnector	☐Storage ☐Supplier ☐System Operator ☐Transmission Owner ☐Virtual Lead Party ☐Other

I wish my response to be:

(Please mark the relevant box)

☒ **Non-Confidential** *(this will be shared with industry and the Panel for further consideration)*

☐ **Confidential** (this *will be disclosed to the Authority in full but, unless specified, will not be shared with the Workgroup, Panel or the industry for further consideration)*

For reference the Applicable CUSC (charging) Objectives are:

a) *That compliance with the use of system charging methodology facilitates effective competition in the generation and supply of electricity and (so far as is consistent therewith) facilitates competition in the sale, distribution and purchase of electricity;*

b) *That compliance with the use of system charging methodology results in charges which reflect, as far as is reasonably practicable, the costs (excluding any payments between transmission licensees which are made under and accordance with the STC) incurred by transmission licensees in their transmission businesses and which are compatible with standard licence condition C11 requirements of a connect and manage connection);*

c) *That, so far as is consistent with sub-paragraphs (a) and (b), the use of system charging methodology, as far as is reasonably practicable, properly takes account of the developments in transmission licensees' transmission businesses and the ISOP business*;*

d) *Compliance with the Electricity Regulation and any relevant legally binding decision of the European Commission and/or the Agency **; and*

e) *Promoting efficiency in the implementation and administration of the system charging methodology.*

** See Electricity System Operator Licence*

***The Electricity Regulation referred to in objective (d) is Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (recast) as it has effect immediately before IP completion day as read with the modifications set out in the SI 2020/1006.*

Please express your views in the right-hand side of the table below, including your rationale.

<table>
<tr><th colspan="3">Standard Workgroup Consultation questions</th></tr>
<tr><td rowspan="3">1</td><td rowspan="3">Do you believe that the Original Proposal and better facilitates the Applicable Objectives?</td><td>Mark the Objectives which you believe the Original solution better facilitates:</td></tr>
<tr><td>Original ☒A ☒B ☒C ☐D ☒E</td></tr>
<tr><td>Yes.

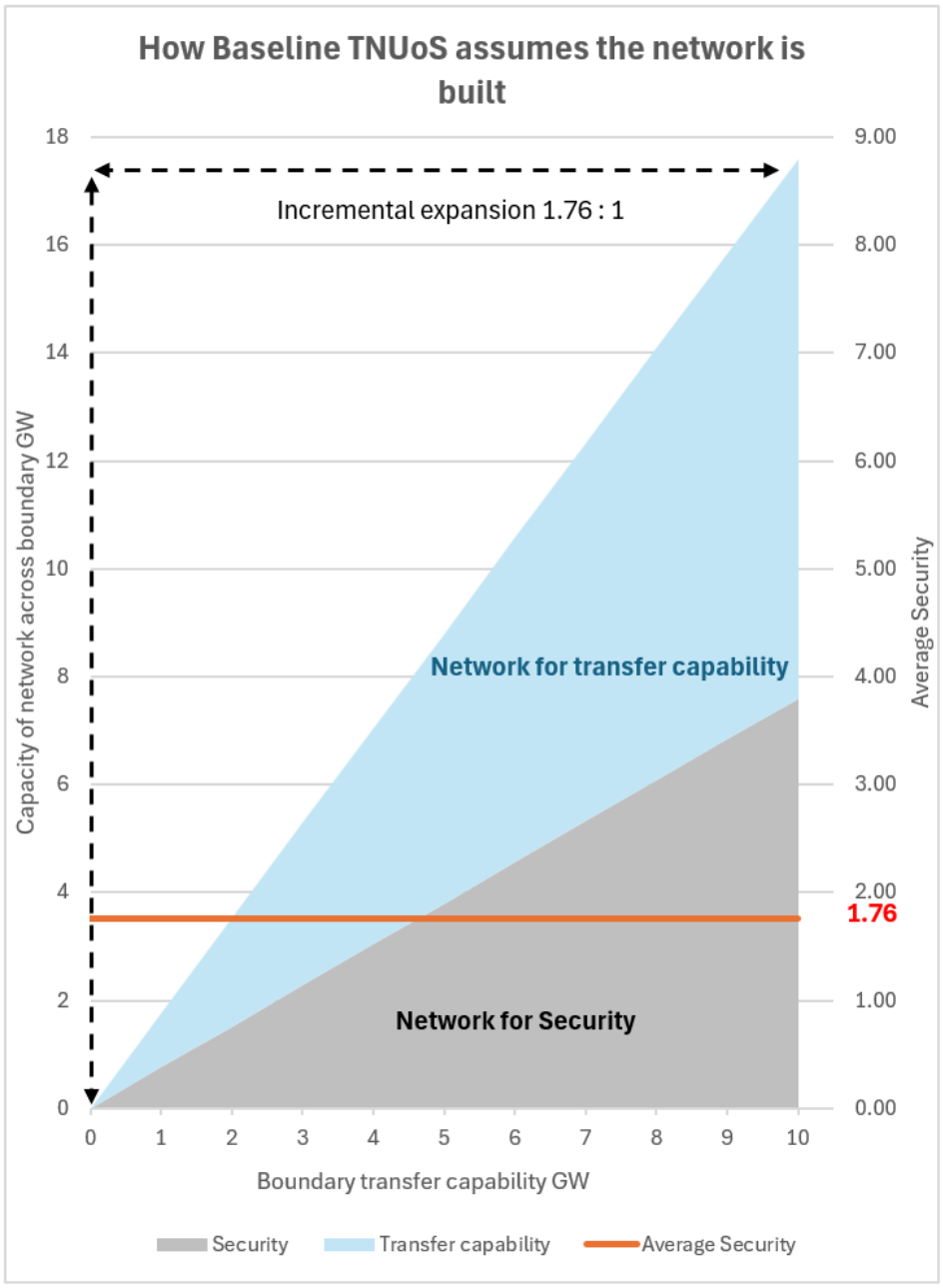
A “Effective competition”: Yes. Removing Security Factor would be better for effective competition for both Generators and demand through: Firstly, deliver better predictability of Wider locational TNUoS charges, for both Generators and demand, by reducing the sensitivity of charges to changes in elements such as: Expansion Constant, Expansion Factors, or location of generation, demand and new network. Currently, the impact on charges from</td></tr>
</table>

		changes in any of these elements is amplified by multiplying their impact by the 1.76 Security Factor. Secondly improve international competition for Generators because the Security Factor would nolonger inappropriately amplify the cost of network charges compared with the network charges paid by Generators in other markets. B “Cost reflectivity”: Yes. Removing the Security Factor would be better for cost reflectivity for both Generator and demand charges. This is because the change would result in Wider locational TNUoS charges that better reflect the cost of incremental network investment. C “Developments in transmission business”: Yes. As the planned growth of the Transmission network increases to meet net zero, it is becoming increasingly apparent that such new network is being built for economic reasons to increase power transport capacity. t is increasingly clear that such new network investment is not being built with accompanying pro-rata additional surplus redundant network capacity for security purposes. D “Electricity Regulation”: Neutral E “Efficient implementation and administration”: Yes. Removing the Security Factor calculation and its application to Wider charges would make the administration of the charging methodology more efficient by removing the need for NESO to operate the Secure Load Flow model (SECULF) that is currently used to calculate the Security Factor or implement its results into the charging methodology.
2	Do you support the proposed implementation approach?	☒Yes ☐No Click or tap here to enter text.
3	Do you have any other comments?	This proposal will likely deliver a number of benefits to customers, which should be modelled in further detail. These include: **Cheaper CfD Strike Prices:** Cheaper TNUoS cost for northern low carbon generation will likely reduce the clearing price of CfD AR7 and beyond. This will enable

		more low carbon generation to be procured at a lower cost to customers of achieving CP30 and Net Zero. **Cheaper Capacity Mechanism clearing prices:** Cheaper TNUoS costs for northern Capacity Mechanism eligible generation, is likely to reduce the clearing price of the Capacity Mechanism, hence reduce the cost of securing capacity for customers. **Cheaper total system cost, which is likely to lead to lower costs to customers:** This proposal will result in TNUoS charges that are more cost reflective, therefore, in as far as generators are able to usefully respond to TNUoS locational price signals, should tend to better facilitate more economically efficient locational investment decisions. **No distributional impact between generation and demand:** It is likely that from circa 2030 onwards, the total collected from each of generation and demand will be restricted by the 2.50 Euro cap (limiting regulation 838/2010) irrespective of whether this modification is approved, or not. So, from that time onwards, this modification will have no impact on the share of TNUoS paid by demand, so would not cause any longer-term redistribution of TNUoS costs between generation and demand.
4	Do you wish to raise a Workgroup Consultation Alternative Request for the Workgroup to consider?	☐Yes (the request form can be found in the Workgroup Consultation Section) ☒No
		Not at this time.
5	Do you agree with the Workgroup's assessment that the modification does not impact the Electricity Balancing Regulation (EBR) Article 18 terms and conditions held within the Code?	Yes

Specific Workgroup Consultation questions		
6	Do you think there are any other approaches to reflecting the cost of security or is there a value other than 1 or 1.76 that is more appropriate. If you have any supporting evidence, please provide this?	No, we do not think any other approaches, or values would be appropriate. The appropriate cost reflective value of the Security Factor is "1.00" to apply to the MWkm for Wider tariffs. Given that it is redundant to multiply tariffs by a factor of "1.00", it is therefore appropriate to remove the Security Factor from the Wider tariff calculation entirely. **The SECULF model, that derived 1.76 for the wider tariffs, does not provide an appropriate measure of what a Security Factor should be.** The approach employed by the Locational Security Factor does not reflect the cost of security. From the TNUoS Locational Onshore Security Factor Calculation Guidance Document it states the purpose of the factor is to *'consider the additional redundancy that is built into the network through the obligation on the Transmission Owners (TOs) to meet the SQSS requirements, and to accommodate flows under both planned and unplanned circuit outages.'* However, TOs plan network expansion using Section 4 of the SQSS, applying different generation backgrounds and specific outage conditions. In Scotland, they use n-1 or n-D criteria, while in England and Wales, they also check for stability with n-2 scenarios. If the network passes these tests without operability or stability issues and the largest circuit loss is within the 1.8GW limit, then no additional MITS reinforcement is needed to increase security alongside any increase in network transfer capacity. By contrast, the security factor implies a requirement to build 1.76 times any required increase in transfer capability, which is not representative of network planning practices.
7	Do you believe price signals should reflect	Price signals should reflect incremental cost. This may include a form of average incremental cost, such as in cases where it is not practically possible to attribute the cost of individual network elements to specific network users, such as in a shared and meshed network.

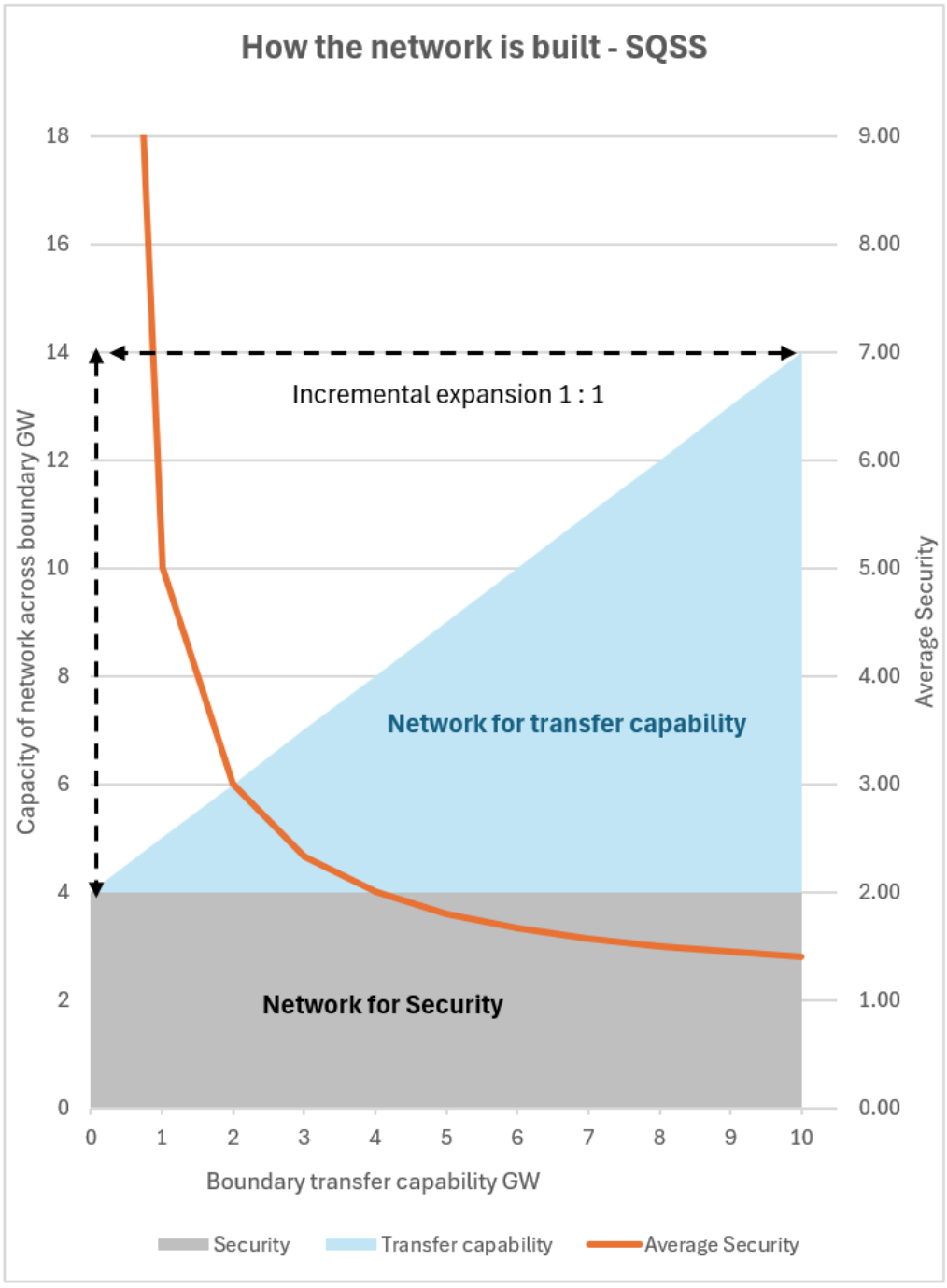
	average existing cost, incremental cost, a combination of the 2, or something else?	By contrast, price signals should not reflect average existing cost, where that would include sunk costs, or fixed costs that do not vary with network expansion. The difference between sunk cost and incremental cost can be understood in the illustrative graphs below. The Y-axis shows the total thermal capacity of circuits crossing any given boundary. The X-axis shows the boundary transfer capability of the same boundary. The Y-axis on the right-hand side shows the average security which is the Y-axis divided by the X-axis. The Baseline TNUoS methodology incorrectly assumes that the cost of security always increases proportionately with the expansion of network transfer capacity. It does this by incorrectly charging the current average level of security as if it is an incremental cost, which it is not. The graph below illustrates how the Baseline charging methodology incorrectly assumes that security is provided in proportion to network expansion.



The graph above shows the network capacity increasing in a 1.76:1 ratio, reflecting the current SECULF security factor. The security portion reflects the 0.76 security increase, while the network for transfer capability shows the remaining 1.

The red line is a constant as the model always assumes an increase in the thermal capacity by a factor of 1.76 above what is needed by the boundary transfer capability.

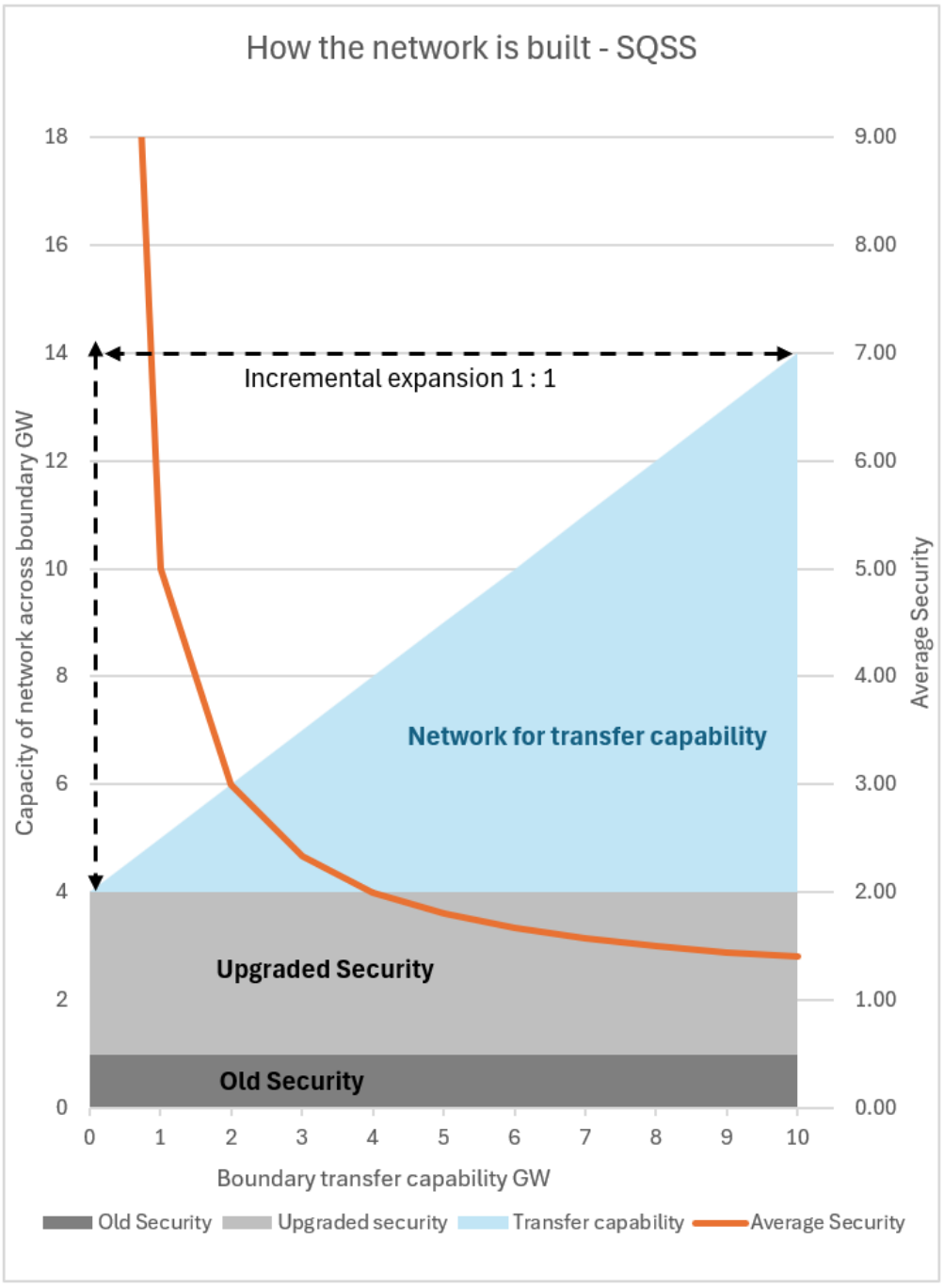
		By contrast, the Original proposal more appropriately separates out the sunk cost of security in the existing network, so that only the incremental cost of security is applied to price signals reflecting the incremental cost of expansion. This results in a more reflective Security Factor of “1.00” as illustrated in the graph below.



The red line shows the average security, which decreases as you build more network, and the boundary transfer capability increases.

As part of the GB societal objective to deliver CMP30 and Net Zero, a decision has been made to upgrade the level of security in some parts of the network, such as northern Scotland, in order to be able to accommodate the growth of

		renewable generation in that area. In this case, the upgrading of security from an old low level to a new higher level, with an increase in size of the fault condition reflects a one-off step change increase in the security level of the network. This cost of upgrading security is a sunk cost because this cost will not vary with the degree of expansion of the network to accommodate more, or less renewables generation in the future. Therefore, the appropriate incremental Security Factor remains “1.00” for such areas of the network upgrade. This step-change increase in security is illustrated in the graph below.



The graph shows that strategic planning will deliver the network up to the same level as the rest of the GB system. As that is decided and approved by Ofgem, security can be treated as a sunk cost, similar to the existing network security.

8	Do you have a view on whether the SECULF model is appropriate? Is enough information available to market participants?	The SECULF model is not appropriate for calculating an incremental Security Factor, so the result of the SECULF model can be disregarded for the purposes of this modification. It is our view that this modification can be approved based on the information that is already available, and this modification should not be contingent on receiving any additional information regarding SECULF from NESO. However, industry currently does not have enough information to understand, peer review, or produce forecasts based on the SECULF model, which places industry in a serious detrimental situation with regards to the Baseline methodology. It would therefore be good practice and better value for customers for NESO to provide much better transparency regarding the SECULF model, as well as much better transparency regarding any other similar models, or processes that NESO may use that also have a large commercial impact on market participants. **1. Why SECULF is not appropriate** **<u>SECULF model does not reflect how security is provided in the current system</u>** SECULF does not measure the degree of average security on the existing network, but instead effectively assumes its own answer of average security based on outdated principles that no-longer apply to the way the network is built for security. The SECULF model is outdated and does not align with current network planning processes. Originally developed around 1992 (33 years ago), to reflect a network driven by conventional generation to serve peak demand without a strategic plan or legislative mandate. It is now inadequate and does not reflect the way the network is planned and built today. With the imperative to achieve NetZero by 2050, strategic planning has become essential. This shift is endorsed by the UK's Electrical Network Commissioner, directed by Ofgem, and implemented by NESO. Network development has evolved from merely accommodating generation to strategically planning for society's energy needs from decarbonised sources. Consequently, if a security factor were to be retained and calculated based on a NESO modelling process, then the SECULF model would require a thorough review to ensure its methodology aligned with latest

		security planning practise. However, since the appropriately reflective result of a properly functioning model would be a security factor of "1.00", then the model process would be redundant, and it would be an inefficient use of NESO resources to develop and operate a new model. **<u>SECULFs attempt to measure average security is not appropriate for providing an incremental investment signal</u>** Incremental investment signals should be based on incremental cost. By contrast, the average level of security on the existing network includes sunk costs and fixed costs that do not vary with network expansion and should not be part of an incremental signal. Therefore, even if the SECULF model were an accurate reflection of existing security, which it is not, then its result would still not be relevant for calculating incremental TNUoS price signals and the result of the SECULF model should be ignored for charging purposes. **2. There isn't enough information and why that's important** We don't believe that using a security factor of greater than 1 is reflective of the incremental cost of network investment, or that not having access to the model undermines this proposal. None the less the model currently used appears flawed. The challenge is that without access to the model, it is impossible to verify what the model is doing in practice, how sensitive it is to the choice of detailed methodology, or input assumptions, or how the result of the model may change with changing input assumptions in the future. The following are some of flaws identified with the model. **<u>What are the SECULF flaws?</u>** 1. The SECULF model restricts flows according to circuit capacity, whereas the DCLF (Transport) model does not, so immediately there is a mix of conflicting signals. 2. The Model works out the worst case scenario for every circuit. It is modelling a doomsday scenario for every circuit and then calculating redundancy needs on the back of this. This is contrary to how the system is planned by TOs using the SQSS. 3. Results are skewed for Scotland. The security requirement is calculated as a MWkm value. In Scotland where there is less redundancy, taking out certain circuits will lead to the MWkm taking long winding routes to get from North to South, often down the only route which has spare capacity which is the HVDC link. Flows must travel East to West and then down to North Wales and back into England. As security is shown as a MWkm figure, if the incremental 1MW can only travel down the longest indirect route then this potentially skews the final answer.

		4. The model outputs are affected by subjective NESO judgements. The final results from the model can and do produce nodes with outlier results. Results for security requirements can range from being close to zero all the way to above 20. In these situations, the NESO uses its experience to disregard certain nodes so as not to skew the results. This is a subjective assessment, which is hard or impossible to replicate and is open to inconsistencies. The subjective assessment is undertaken as in reality the TO's would not provide Security as high as the SECULF methodology suggests is needed, because it's not economic or efficient. 5. Key inputs required that are also not publicly available. The Model requires a" Trip List" from the Control Room in the System Operator to work. This list details a combination of circuits or scenarios to secure against, which can be combinations of up to 5 circuits. The model does not just remove one circuit and then calculate the impact but removes a number of circuits at once. Without this list it is impossible for Industry to replicate the results. We are therefore in a situation where we have a methodology and a model which has not changed since 2001, despite numerous changes to the SQSS and the DCLF Model. We have a model which produces outlier results and uses information not available to Industry, and we have end results which are then modified in ways that are not transparent to network users.