

CMP432 Improve Locational Onshore Security Factor for TNUoS Wider Tariffs

Workgroup 1 (29 January 2025)

Online Meeting via Teams

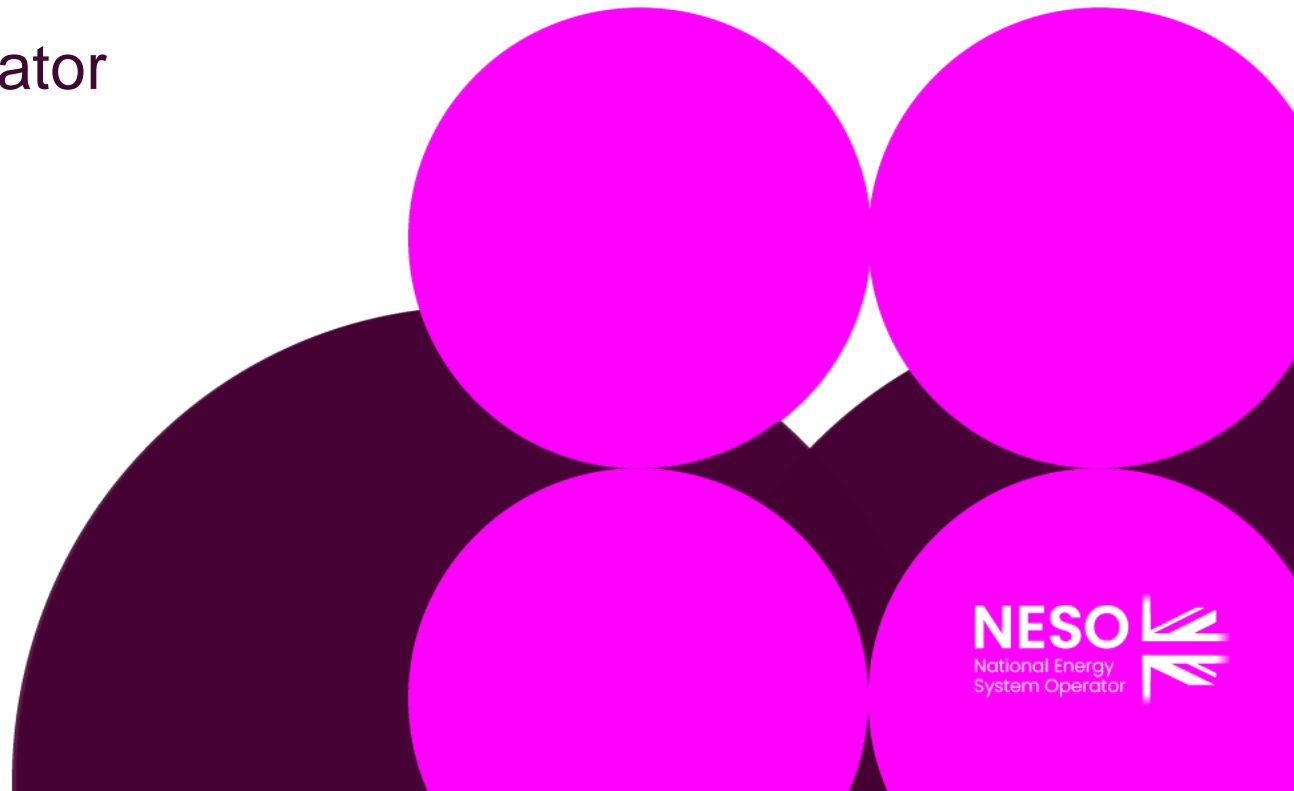
WELCOME

Agenda

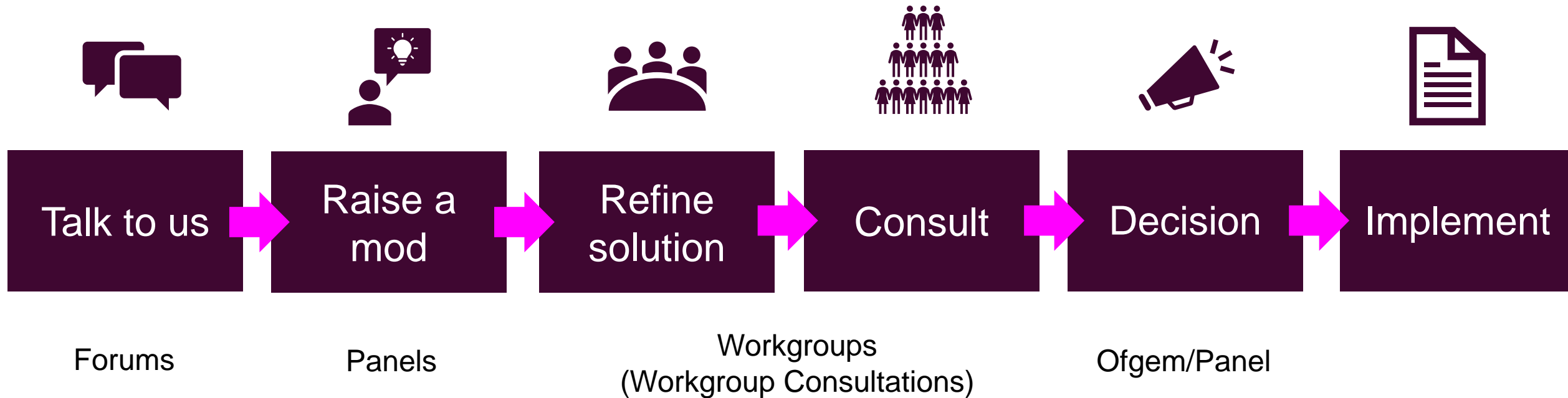
Topics to be discussed	Lead
Introductions	Chair
Code Modification Process Overview <ul style="list-style-type: none">• Workgroup Responsibilities• Workgroup Alternatives and Workgroup Vote	Chair
Objectives and Timeline <ul style="list-style-type: none">• Walk-through of the timeline for the modification	Chair
Review Terms of Reference	All
Proposer presentation	Proposer
Questions from Workgroup Members	All
Agree Terms of Reference	All
Cross Code Impacts	All
Any Other Business	Chair
Next Steps	Chair

Modification Process

Sarah Williams – NESO Code Administrator



Code Modification Process Overview



Refine Solution Workgroups



- If the proposed solution requires further input from industry in order to develop the solution, a Workgroup will be set up.
- The Workgroup will:
 - further refine the solution, in their discussions and by holding a **Workgroup Consultation**
 - Consider other solutions, and may raise **Alternative Modifications** to be considered alongside the Original Modification
 - Have a **Workgroup Vote** so views of the Workgroup members can be expressed in the Workgroup Report which is presented to Panel

Consult Code Administrator Consultation

- The Code Administrator runs a consultation on the **final solution(s)**, to gather final views from industry before a decision is made on the modification.
- After this, the modification report is voted on by Panel who also give their views on the solution.



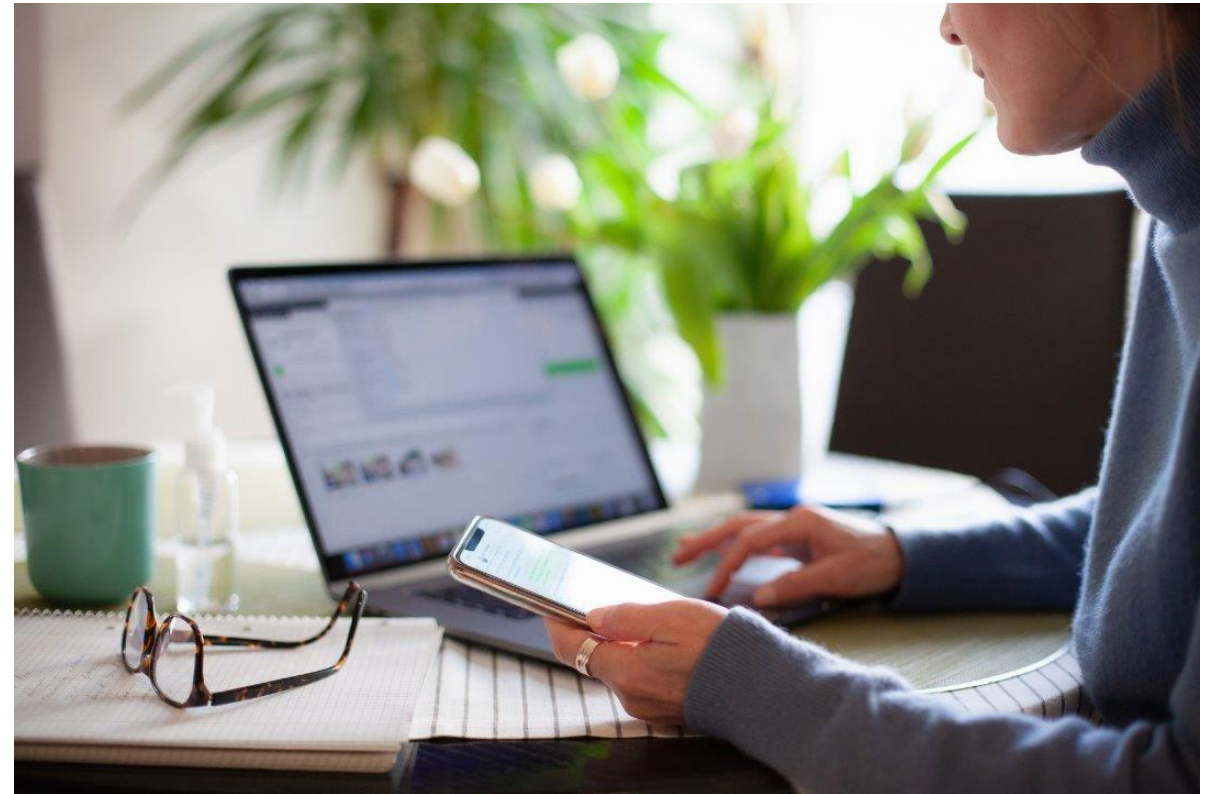
Decision



- Dependent on the Governance Route that was decided by Panel when the modification was raised
- **Standard Governance:** Ofgem makes the decision on whether or not the modification is implemented
- **Self-Governance:** Panel makes the decision on whether or not the modification is implemented
 - an appeals window is opened for 15 days following the Final Self Governance Modification Report being published

Implement

- The Code Administrator implements the final change which was decided by the Panel / Ofgem on the agreed date.



Workgroup Responsibilities and Membership

Sarah Williams – NESO Code Administrator

Public Expectations of a Workgroup Member

Contribute to the discussion

Be respectful of each other's opinions

Language and Conduct to be consistent with the values of equality and diversity

Do not share commercially sensitive information

Be prepared - Review Papers and Reports ahead of meetings

Complete actions in a timely manner

Keep to agreed scope

Email communications to/cc'ing the .box email

Your Roles

Help refine/develop the solution(s)

Bring forward alternatives as early as possible

Vote on whether or not to proceed with requests for Alternatives

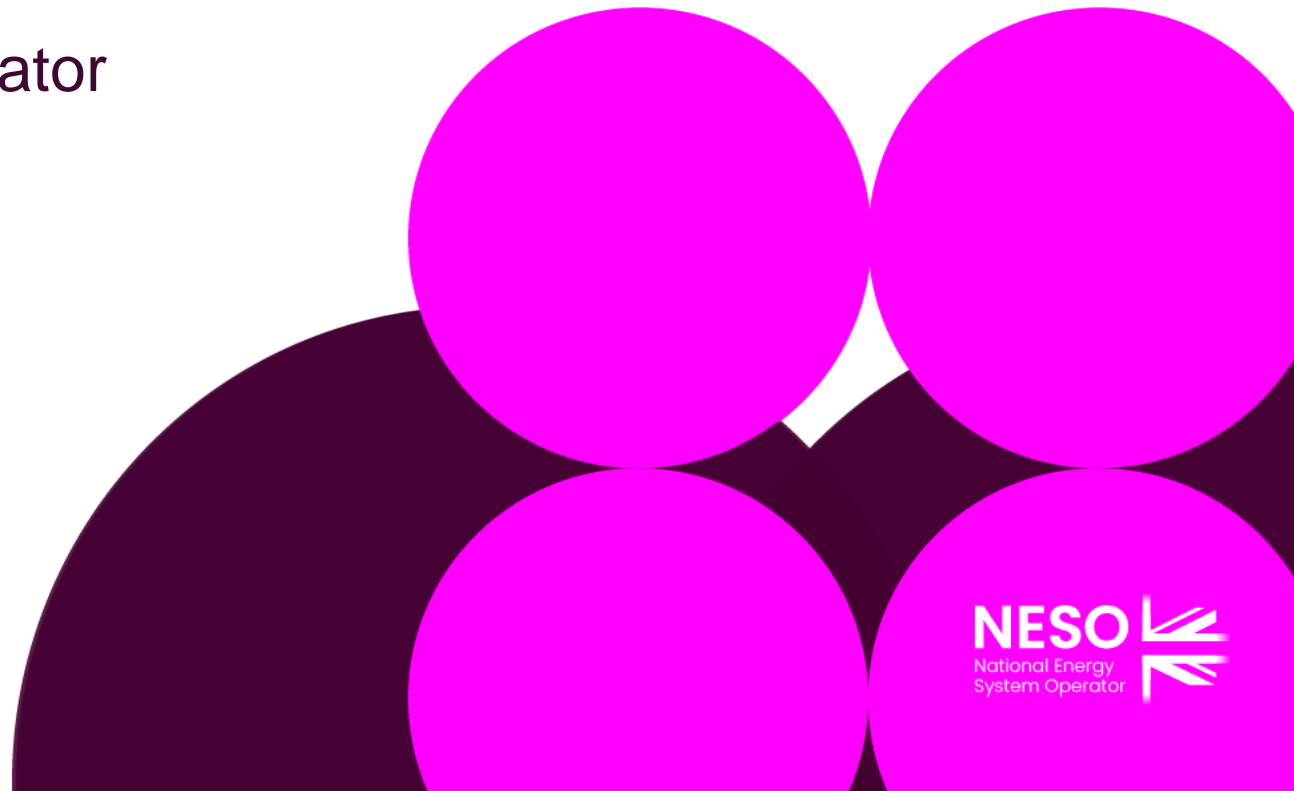
Vote on whether the solution(s) better facilitate the Code Objectives

Workgroup Membership

Role	Name	Company	Alternate	Name
Chair	Sarah Williams	NESO		
Tech Sec	Prisca Evans	NESO		
Proposer	John Tindal	SSE	Alternate	Damien Clough
Workgroup Member	Neil Dewar	NESO		
Workgroup Member	Tom Steward	RWE	Alternate	Lauren Jauss
Workgroup Member	Ryan Ward	Scottish Power Renewables	Alternate	Hector Eduardo Perez
Workgroup Member	Andrew Rimmer	Engie	Alternate	Simon Lord
Workgroup Member	Paul Jones	Uniper	Alternate	Sean Gauton
Workgroup Member	Alan Kelly	Corio Generation	Alternate	Dan Gilbert
Workgroup Member	Giulia Licocci	Ocean Winds		
Observer	Loukas Papageorgiou	RWE		
Observer	Kyle Murchie	Roadnight Taylor	Alternate	Catherine Cleary
Observer	Sally Young	SSE		
Observer	Zahira Rafiq	NESO		
Authority Representative	Sinan Kufeoglu	OFGEM		

Workgroup Alternatives and Workgroup Vote

Sarah Williams – NESO Code Administrator



What is the Alternative Request?

What is an Alternative Request? The formal starting point for a Workgroup Alternative Modification to be developed which can be raised up until the Workgroup Vote.

What do I need to include in my Alternative Request form? The requirements are the same for a Modification Proposal you need to articulate in writing:

- a description (in reasonable but not excessive detail) of the issue or defect which the proposal seeks to address compared to the current proposed solution(s);
- the reasons why you believe that the proposed alternative request would better facilitate the Applicable Objectives compared with the current proposed solution(s) together with background information;
- where possible, an indication of those parts of the Code which would need amending in order to give effect to (and/or would otherwise be affected by) the proposed alternative request and an indication of the impacts of those amendments or effects; and
- where possible, an indication of the impact of the proposed alternative request on relevant computer systems and processes.

How do Alternative Requests become formal Workgroup Alternative Modifications? The Workgroup will carry out a Vote on Alternatives Requests. If the majority of the Workgroup members or the Workgroup Chair believe the Alternative Request will better facilitate the Applicable Objectives than the current proposed solution(s), the Workgroup will develop it as a Workgroup Alternative Modification.

Who develops the legal text for Workgroup Alternative Modifications? ESO will assist Proposers and Workgroups with the production of draft legal text once a clear solution has been developed to support discussion and understanding of the Workgroup Alternative Modifications.

Can I vote? And What is the Alternative Vote?

To participate in any votes, Workgroup members need to have attended at least 50% of meetings. The vote shall be decided by simple majority of those present at the meeting at which the vote takes place (whether in person or by teleconference)

Stage 1 – Alternative Vote

- Vote on whether Workgroup Alternative Requests should become Workgroup Alternative CUSC Modifications.
- The Alternative vote is carried out to identify the level of Workgroup support there is for any potential alternative options that have been brought forward by either any member of the Workgroup OR an Industry Participant as part of the Workgroup Consultation.
- **Should the majority of the Workgroup OR the Chair believe that the potential alternative solution may better facilitate the CUSC objectives than the Original then the potential alternative will be fully developed by the Workgroup with legal text to form a Workgroup Alternative CUSC modification (WACM) and submitted to the Panel and Authority alongside the Original solution for the Panel Recommendation vote and the Authority decision.**

Can I vote? And What is the Alternative Vote?

To participate in any votes, Workgroup members need to have attended at least 50% of meetings. The vote shall be decided by simple majority of those present at the meeting at which the vote takes place (whether in person or by teleconference)

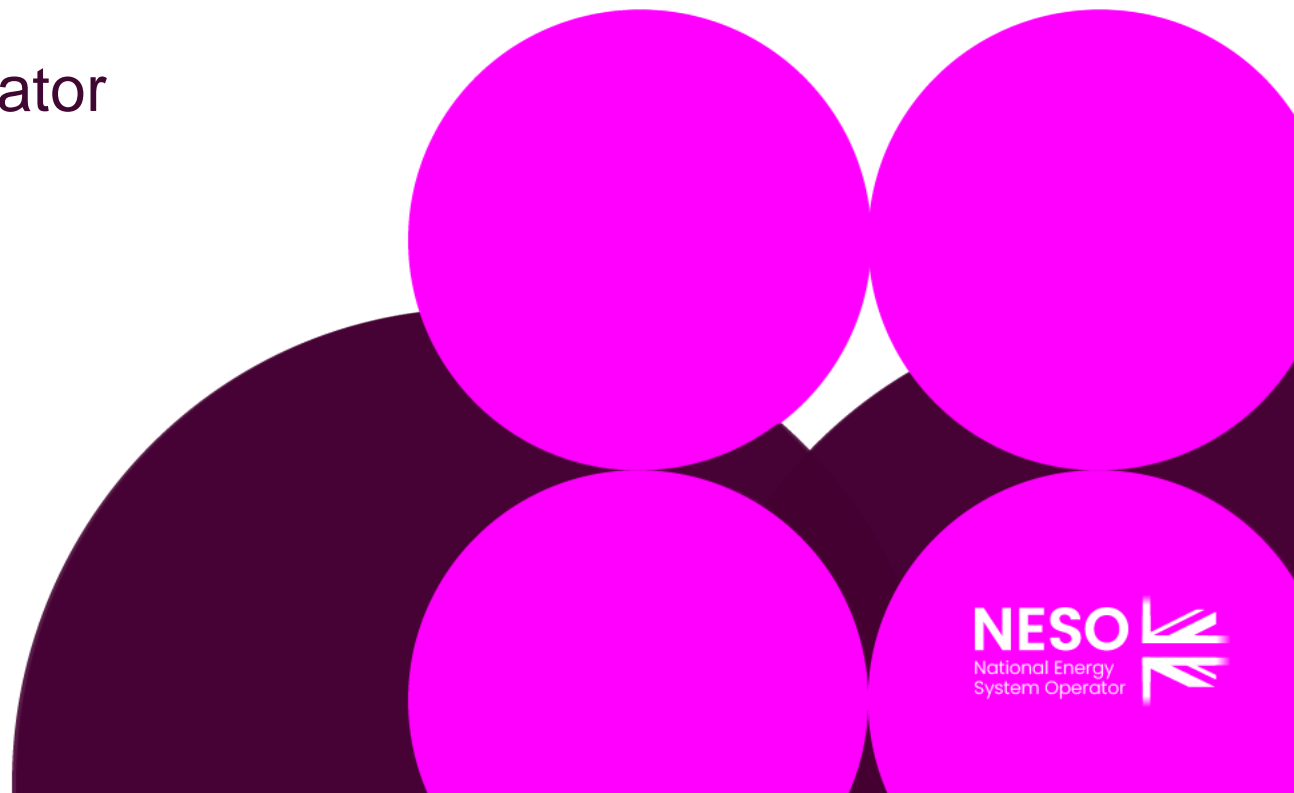
Stage 2 – Workgroup Vote

- 2a) Assess the original and Workgroup Alternative (if there are any) against the relevant Applicable Objectives compared to the baseline (the current code)
- 2b) Vote on which of the options is best.

Alternate Requests cannot be raised after the Stage 2 – Workgroup Vote

Objectives and Timeline

Sarah Williams – NESO Code Administrator



Public Timeline for CMP432 as of 29 January 2025

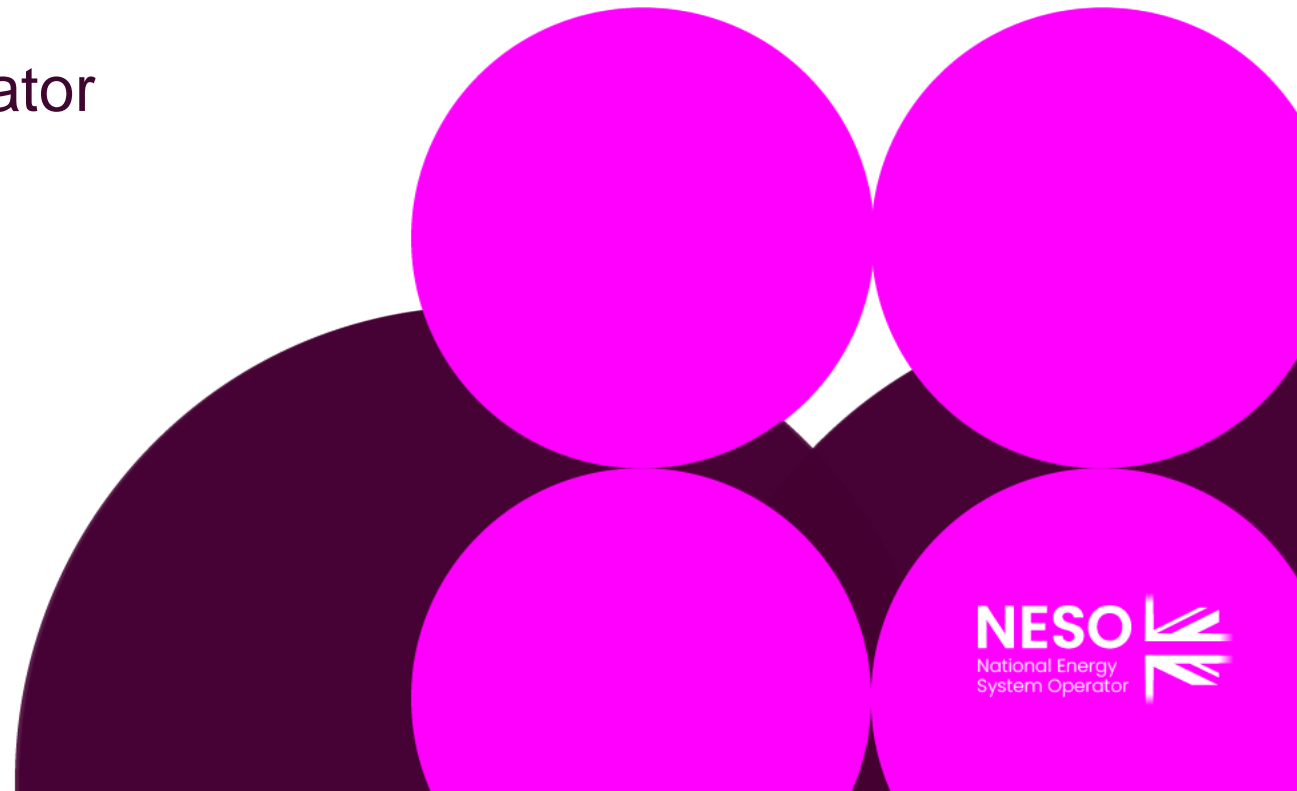
Pre-Workgroup		
Proposal raised	07/03/2024	
Proposal submitted to Panel	22/03/2024	
Workgroup Nominations	09/04/2024	
Urgency Decision Granted	21/01/2025	
Workgroups		
Workgroup 1	29/01/2025	Objectives and Timeline/Review and Agree Terms of Reference / Proposer presentation
Workgroup 2	05/02/2025	Solution Development / Workgroup Discussions/Legal Text
Workgroup 3	14/02/2025	Draft Legal Text/Draft Workgroup Consultation /Specific Questions
Workgroup 4	21/02/2025	Final Workgroup Consultation Review
Workgroup Consultation	26/02/2025 – 06/03/2025	
Workgroup 5	13/03/2025	Review of Workgroup Consultation Responses / Alternative Requests Discussion/Review Solution position
Workgroup 6	20/03/2025	TOR Discussion/Alternative Requests Presentations and Vote (if required)/
Workgroup 7	26/03/2025	Draft Legal text and WACMs Legal text (if required) review
Workgroup 8	03/04/2025	Final Workgroup Report Review / ToR Sign-off / Final Legal Text Review (WACMS legal text)

Timeline for CMP432 as of 29 January 2025

Post Workgroups		Key info
Workgroup Report submitted to Panel	14/04/2025	
Panel to agree whether ToR have been met	17/04/2025	Special Panel invites to be shared
Code Administrator Consultation	22/04/2025 – 02/05/2025	
Code Administrator Consultation Analysis and DFMR generation	02/05/2025 – 08/05/2025	
Draft Final Modification Report to Panel	09/05/2025	
Panel Recommendation Vote	15/05/2025	Special Panel
Final Modification to Ofgem	15/05/2025	
Decision Date	30/09/2025	
Implementation Date	01/04/2026	

Review Terms of Reference

Sarah Williams - NESO Code Administrator



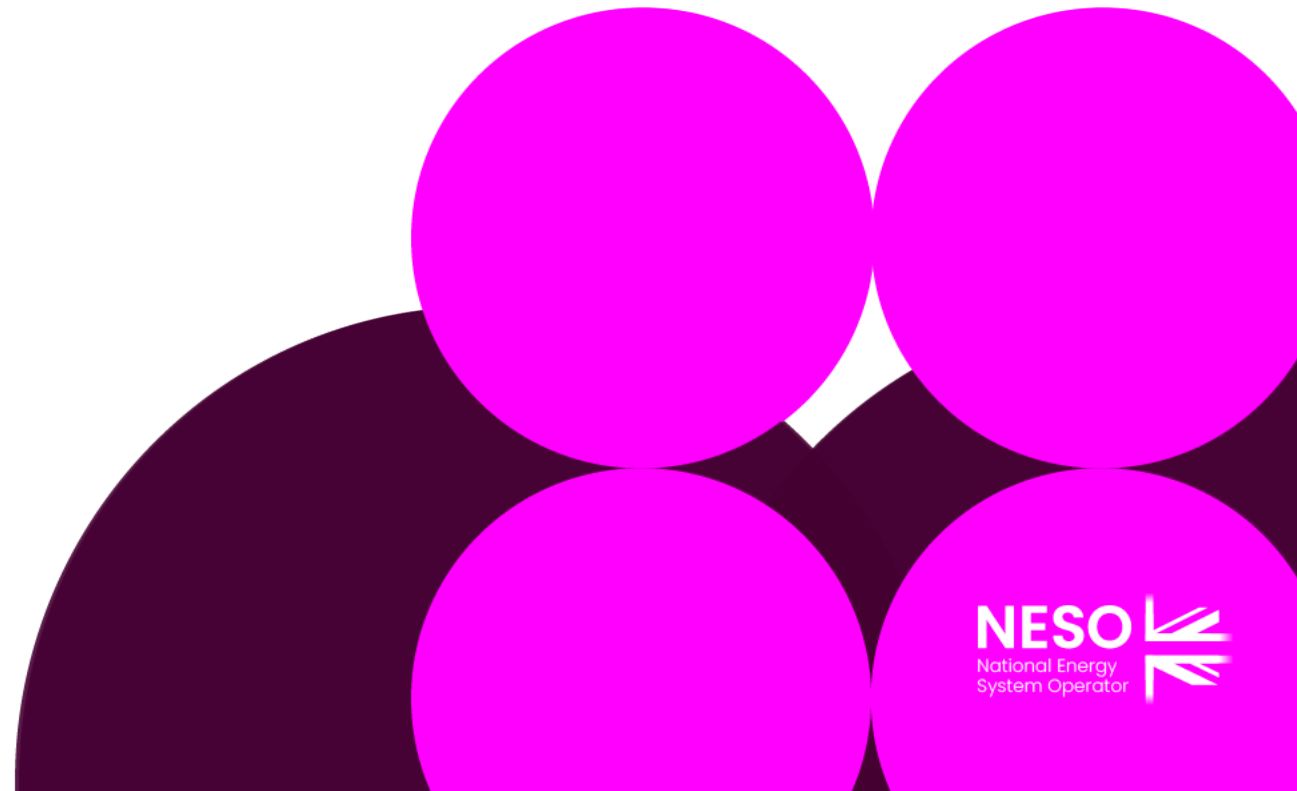
Public

CMP432 - Terms of Reference

Workgroup Term of Reference	Location in Workgroup Report (to be completed at Workgroup Report stage)
a) Consider EBR implications	
b) Consider the methodology for calculating the security factor (Locational Onshore Security Factor Section 14.15.88 – 14.15.90) and the further objectives of the Charging Methodology set out in Section 14. 14.11	
c) Consider whether reinforcement with a larger capacity circuit, compared with the previous, increases the fault condition.	
d) Consider the impact of whether reinforcement is achieved by upgrading an existing circuit to a larger capacity, therefore increasing the fault condition	
e) Consider whether some types of technology require additional MITS redundancy, e.g. large inflexible conventional such as nuclear	
f) Consider and evaluate the evidence that the current Security Factor is reflective of how TOs make network reinforcement decisions	
g) Consider the scope of work identified and whether this is achievable within the timeframe outlined in the Ofgem Urgency decision letter	

Proposer's Solution: Background; Proposed Solution; Scope; and Assessment vs Terms of Reference

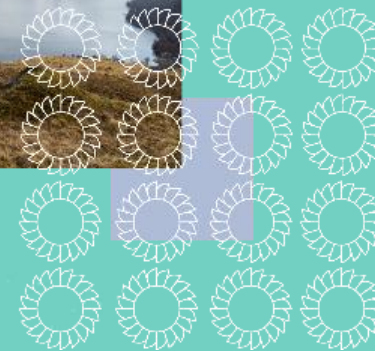
John Tindal – SSE



CUSC Modification Proposal CMP432

Improve "Locational Onshore Security
Factor" for TNUoS Wider Tariffs

January 2025



Contents:

Section 1 – Summary

Section 2 – Explaining the defect

Rationale for TNUoS Charges

*“The underlying rationale behind Transmission Network Use of System charges is that efficient economic signals are provided to Users when services are priced to reflect the **incremental costs** of supplying them.”*

(CUSC 14.14.6 – underlying rationale behind TNUoS Charges)

SQSS requires that MITS Transmission network is already sufficiently secure, so:

...if additional MITS network capacity does not require additional redundancy for security

...Then TNUoS Wider locational price signal should not charge for additional redundancy for security

What is the Proposed Solution ?

Improve the Security Factor from the Transport model

Analysis of SQSS indicates:

- Locational Onshore Security Factor from Wider Tariffs (Peak Security & Year Round) should be = 1.00

Options for amending the CUSC and Transport & Tariff model:

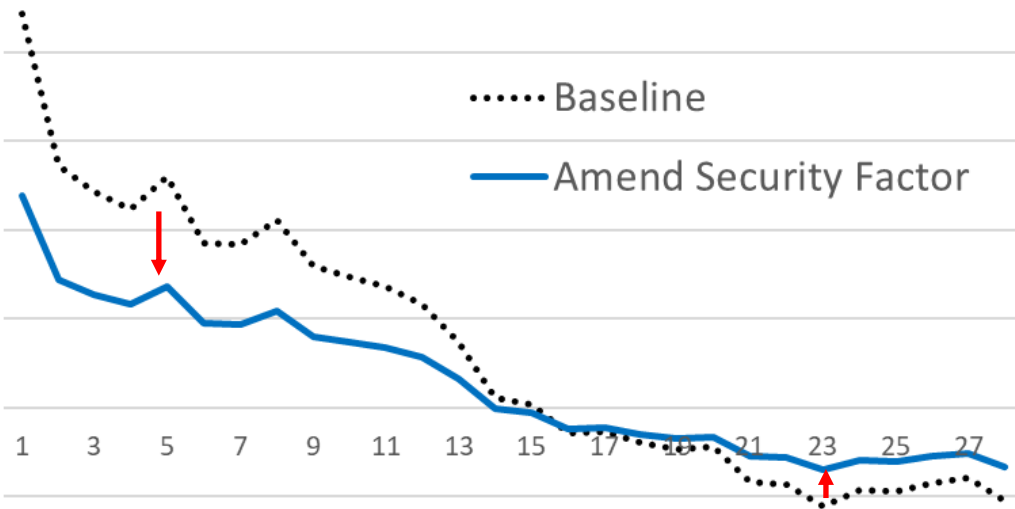
- **OPTION 1:** Remove the Locational Onshore Security Factor entirely from all Wider charges
- **OPTION 2:** Amend the Locational Onshore Security Factor for Wider Tariffs to be 1.00

Note: Local charges remain unchanged, but could be investigated separately

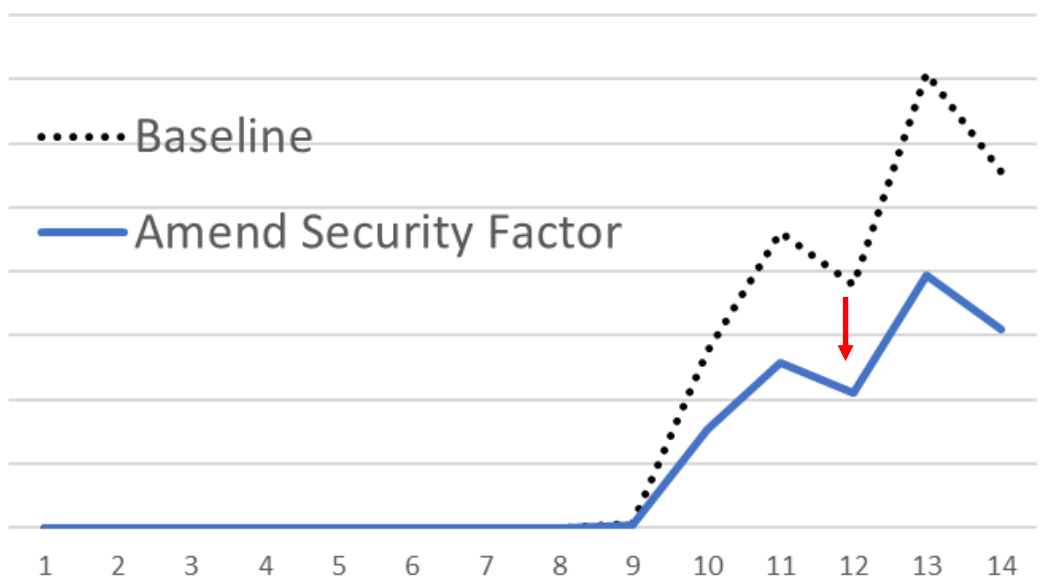
What is the Impact of the Change?

Examples of Charges Before and After Amending the Security Factor

Flatter Gradient for Generator Charges



Flatter Gradient for Demand Charges



Results for Generators:

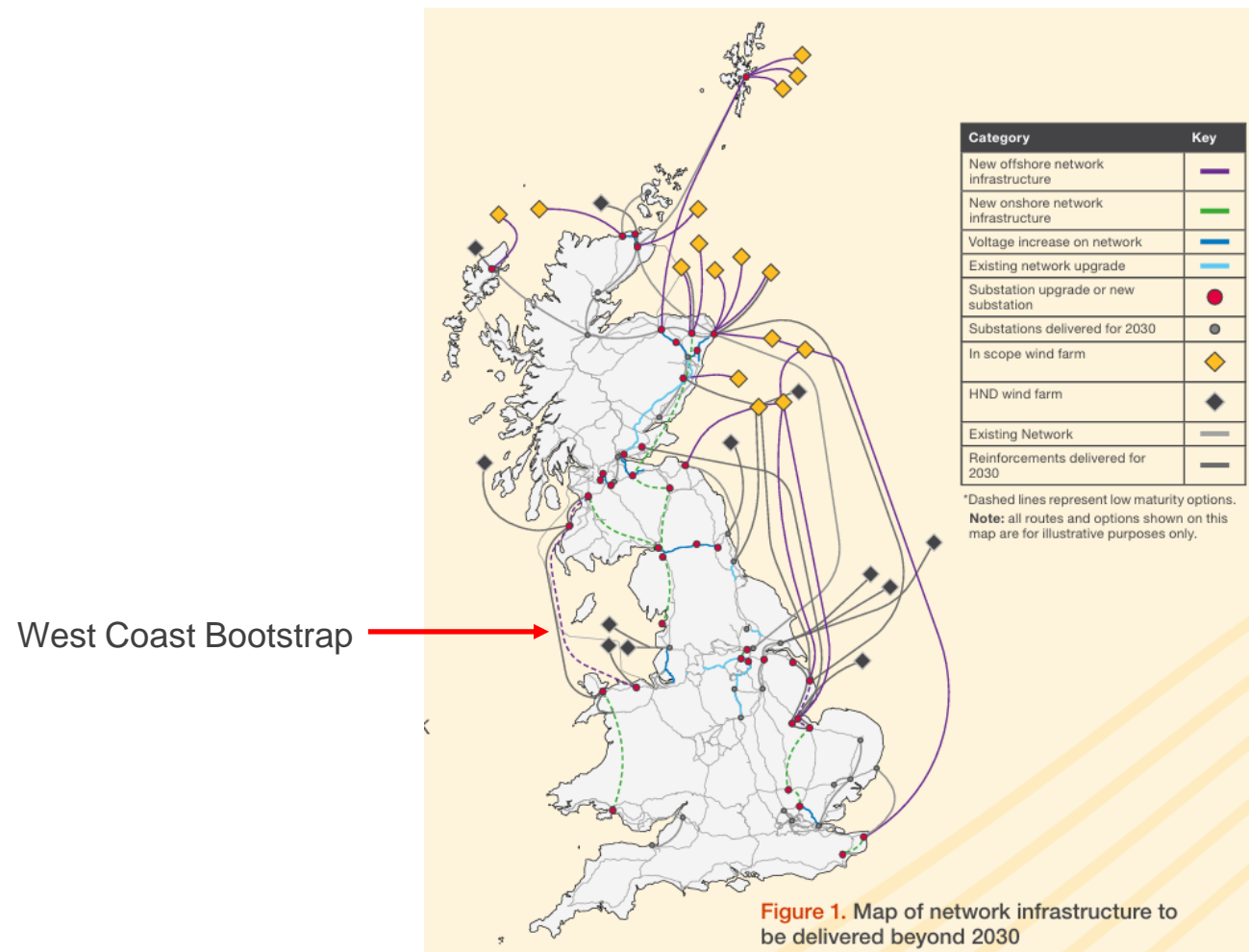
- **Flatter gradient for locational charges:** reduced differential between North & South
- **Reduced magnitude of generator adjustment credit**

Results for Demand

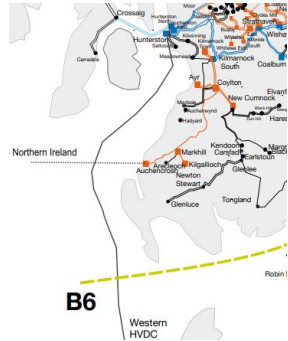
- **Flatter gradient for demand charges:** reduced Southern charges, Northern floored at £zero
- **Higher Demand Residual charges:** smaller collection from demand locational (mitigated by reduced northern demand credits after CMP440)

Examples are for the year 2035. The Generator Charges example is for an intermittent generator, including the effect of the residual change.

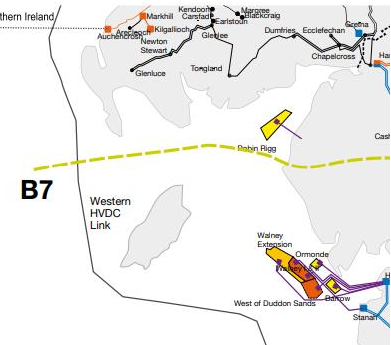
Empirical example: Future incremental network looks a lot like West Coast Bootstrap (Beyond 2030)



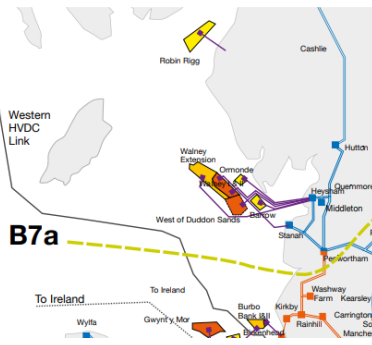
Empirical example: West Coast Bootstrap (ETYS)



- **B6** – ‘the boundary capability has increased to 5.7GW compared to last year due to the addition of the new Western HVDC circuit and upgrade of cables at Torness.’



- **B7** – ‘the boundary capability has increased to 6.5GW compared to last year due to the addition of the new Western HVDC circuit.’



- **B7a** – ‘the boundary capability has increased to 8.7GW compared to last year due to the addition of the new Western HVDC circuit.’

Zone	Boundary Transfer Capability 2017 (GW) ¹	Boundary Transfer Capability 2018 (GW) ²	Change in Boundary Transfer Capability (GW)	Bootstrap Capacity 2018 (GW)	Implied incremental Security Factor 2018
B6	3.5	5.7	2.2	2.2	<u>1.00</u>
B7	4.3	6.5	2.2	2.2	<u>1.00</u>
B7a	6.0	8.7	2.7	2.2	<u>0.81</u>

Additional questions from Terms of Reference “b”

Consider the methodology for calculating the security factor (Locational Onshore Security Factor Section 14.15.88 – 14.15.90)

14.15.88 The locational onshore security factor for everything other than Identified Onshore Circuits is derived by running a secure DCLF ICRP transport study of the network excluding local circuits and Identified Onshore Circuits based on the same market background as used for Zoning in the DCLF ICRP transport model. This calculates the nodal marginal costs where peak net demand can be met despite the Security and Quality of Supply Standard contingencies (simulating single and double circuit faults) on the network. Essentially the calculation of secured nodal marginal costs is identical to the process outlined above except that the secure DCLF study additionally calculates a nodal marginal cost taking into account the requirement to be secure against a set of worse case contingencies in terms of maximum flow for each circuit.

- **SECULF measures existing average conditions, not incremental conditions. If incremental conditions are different, then the SECULF model is irrelevant**
- **SECULF currently uses the Year Round background due to largest flow, but YR background is about bulk energy and CBA trade-off between network vs constraints, not demand security, so wrong background for measuring security**

14.15.89 For the purposes of 14.15.88 the secured nodal cost differential is compared to that produced by the DCLF ICRP transport model and the resultant ratio of the two determines the locational security factor using the Least Squares Fit method. Further information may be obtained from the charging website.

- **The measured ratio of secured to unsecured MWkm is different from redundant network capacity built for security, so the answer does not mean what it claims to mean**

14.15.90 For the purposes of 14.15.88 the locational onshore security factor, derived in accordance with paragraphs 14.15.88 and 14.15.89 and expressed to eight decimal places, is based on an average from a number of studies conducted by The Company to account for future network developments. This security factor is reviewed for each price control period and fixed for the duration. The locational onshore security factor which is currently applicable, is detailed in The Company's Statement of Use of System Charges, which is available from the Charging website.

- **Action: Ask NESO to share the SECULF model, so WG can consider it**
- **Action: Ask NESO publish the historical working calculations behind these studies beyond simply the final answer**

14.15.90A An Identified Onshore Circuit shall be defined as a single transmission HVDC subsea circuit or a single transmission AC subsea circuit between two MITS Nodes where there is only one route for the power to flow between the two MITS Nodes. The expansion factors for Identified Onshore Circuits are adjusted by dividing the applicable expansion factor for the Identified Onshore Circuits, calculated as per Sections 14.15.70 to 14.15.77, by the locational onshore security factor calculated in 14.15.90. When the locational onshore security factor is applied as per Section 14.15.94 and 14.15.95, this would result in an effective locational onshore security factor for Identified Onshore Circuits of 1.0.

- **This solution still has a defect: There may be zero redundancy for security purposes, even if there is more than “one route”. So there is a risk that when a second route is added, that the circuit will cease to be “identified” and its Security Factor will inappropriately (non cost reflective) revert to the standard locational onshore security factor**

Additional questions from Terms of Reference

Further objectives of the Charging Methodology set out in Section 14. 14.11

“14.14.11 In setting and reviewing these charges The Company has a number of further objectives. These are to:

- offer clarity of principles and transparency of the methodology;*
- inform existing Users and potential new entrants with accurate and stable cost messages;*
- charge on the basis of services provided and on the basis of incremental rather than average costs, and so promote the optimal use of and investment in the transmission system; and*
- be implementable within practical cost parameters and time-scales.” [emphasis added]*

➤ **SECULF model measures average, not incremental**

Industry Feedback for consideration – in TOR

Following discussions with TNUoS Task Force, TCMF, ESO

1) What if reinforcement was a larger capacity circuit, compared with the previous, increasing the fault condition ? (TOR “c”)

- If the fault condition increased, much of the new circuit will be held in reserve, so limited benefit from the increased capacity. This naturally limits the capacities of new circuits included in network design, so this is not an issue for long-run price signal.
- There will be occasions when an additional circuit may release **more** transfer capacity than just the specific circuit itself.
- Changing fault conditions should **not** be part of a long-run marginal cost signal.

2) What if reinforcement was achieved by upgrading an existing circuit to a larger capacity, therefore increasing the fault condition? (TOR “d”)

- The decision to upgrade instead of building new (e.g. reconductoring) is primarily driven by ongoing maintenance considerations.
- Also see answer to Question1 above

3) Do some types of technology require additional MITS redundancy, e.g. large inflexible conventional such as nuclear? (TOR “e”)

- Flexible generation, e.g. wind, require relatively low redundancy, as network outages can be managed through constraints and intertrip contracts
- Security Factor could be charged differently between the Peak-Security versus Year-Round backgrounds
- Consider if security should be applied to charges differently for different technologies and/or backgrounds

4) What evidence is there that the current Security Factor is reflective of how TOs make network reinforcement decisions (TOR “f”)

- To be considered by the workgroup
- Action: request WG support from NESO NOA team (or other relevant experts) and Tos

Requests and next steps

1. **Request to NESO and TOs:** Transparency and support to Workgroup regarding how incremental network is planned and built to take account of incremental security. This is because NESO and TO network planning documents do not currently provide:
 - Transparent breakdown between firstly how much incremental network transfer capacity is required and secondly how much incremental redundant network capacity is required for security, then how these inform the incremental cost and capacity of total network that is planned and built to deliver both incremental transfer capacity and incremental security.
 - Support from NESO and TOs to the workgroup will enable the workgroup to better understand the cost of network incurred for incremental security, which TNUoS charges are supposed to reflect
2. **Share with WG new report from consultant**
3. **Request to NESO:** data and models (SECULF) shared with WG
4. **Request to NESO:** Industry access to VBA code within the Transport and Tariff model
5. **Ofgem decision date:** In time for CfD AR7 2025, same as CMP444
6. **Implementation date:** 1st April 2026 (same as originally proposed)

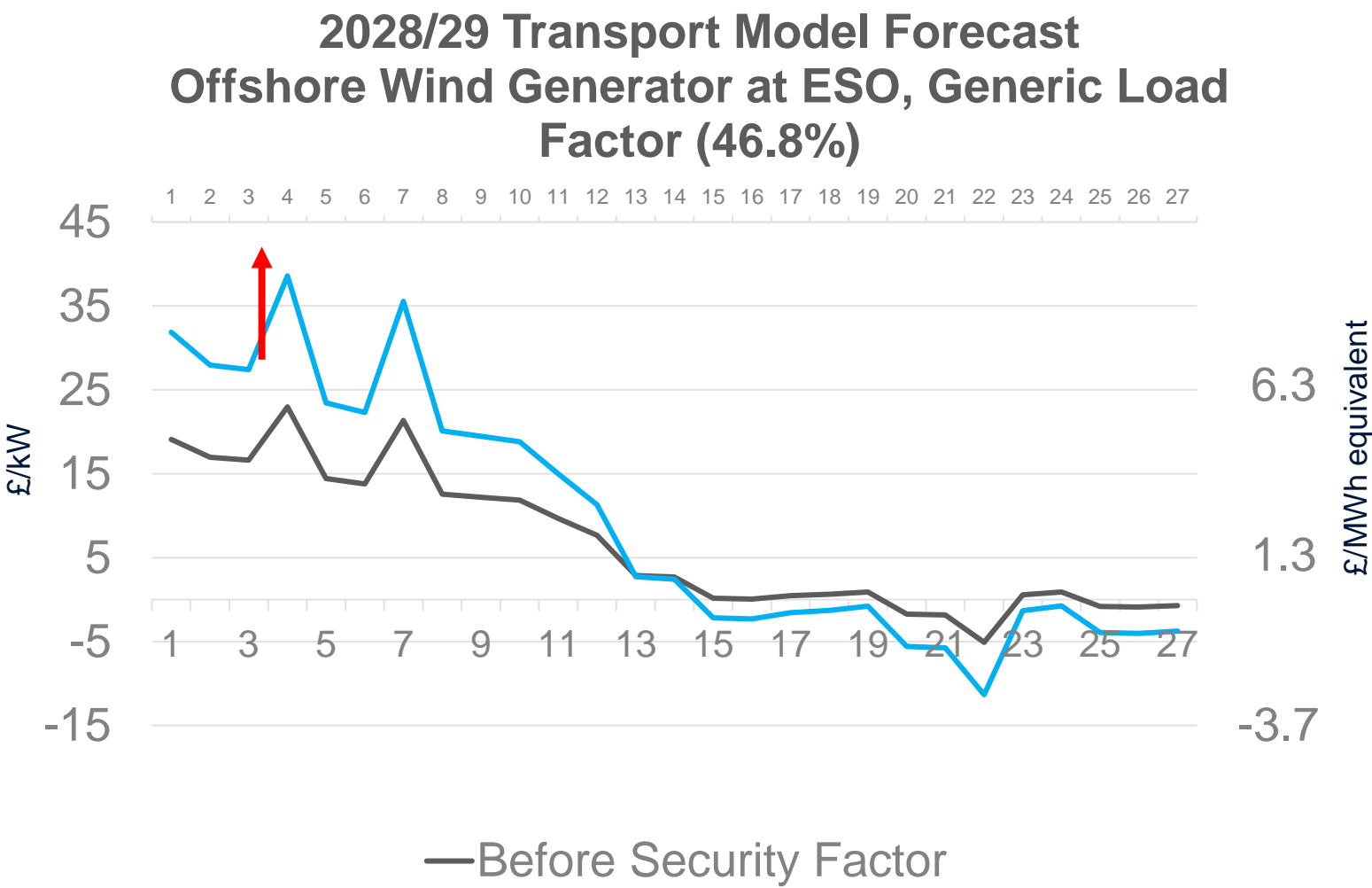
Contents:

Section 1 – Summary

Section 2 – Explaining the defect

Section 3 – Further questions relating to TOR

Security Factor amplifies locational signal



- Security Factor multiplies Wider locational tariffs by 1.76
- Increases Zone 4 charges by £3.85 per MWh (from £5.66 to £9.51 per MWh)
 - Increases Zone 22 credit by £1.53 per MWh (from -£1.26 to -£2.79 per MWh)
 - Max-min spread increases by £5.39 per MWh (from £6.92 to £12.30 per MWh)

Illustrative Reinforcement for Additional Generation

New wind farm:

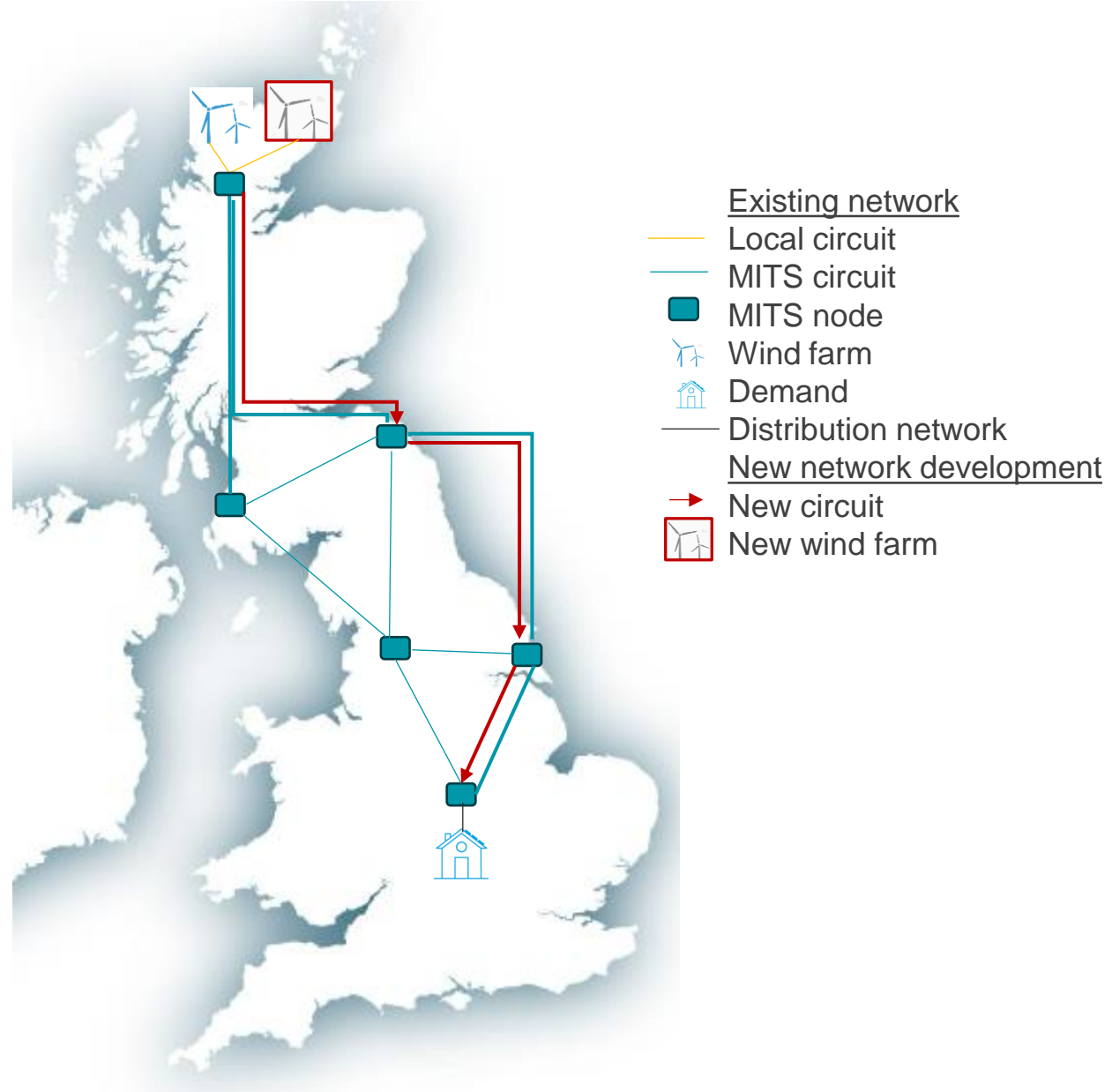
+1GW transfer capacity

Economic reinforcement:

+1GW across the network

Transport model assumes:

+1.76GW across the network



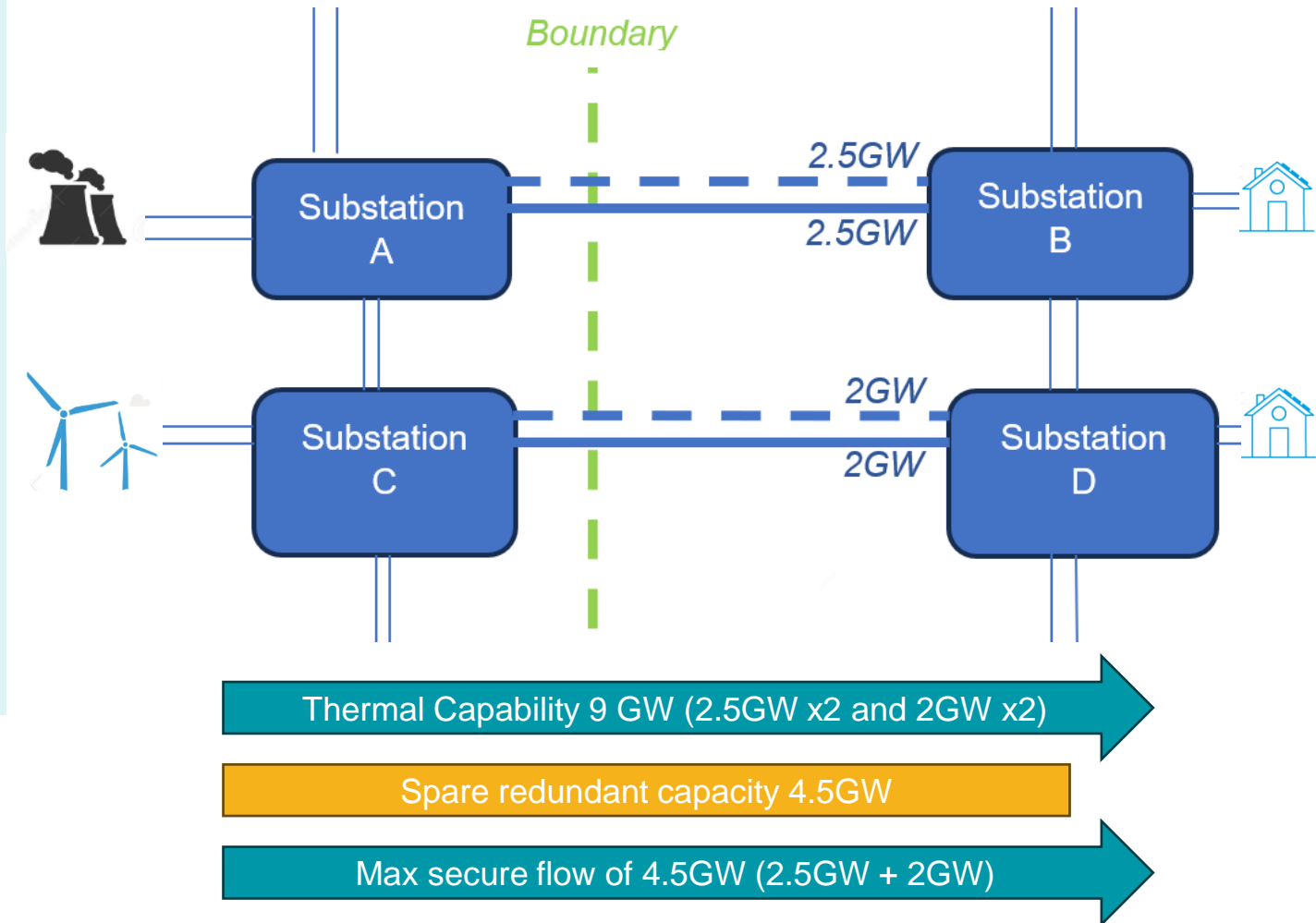
What is the issue?

SQSS says: MTS network is already sufficiently secure

SQSS

TOs plan network additions using SQSS criteria
Surplus capacity is required in case of faults or outages including:

- “N-2” : Outage on two largest separate circuits
- *Boundary is initially secure*



What is the issue?

SQSS says: Want 1GW, build 1GW

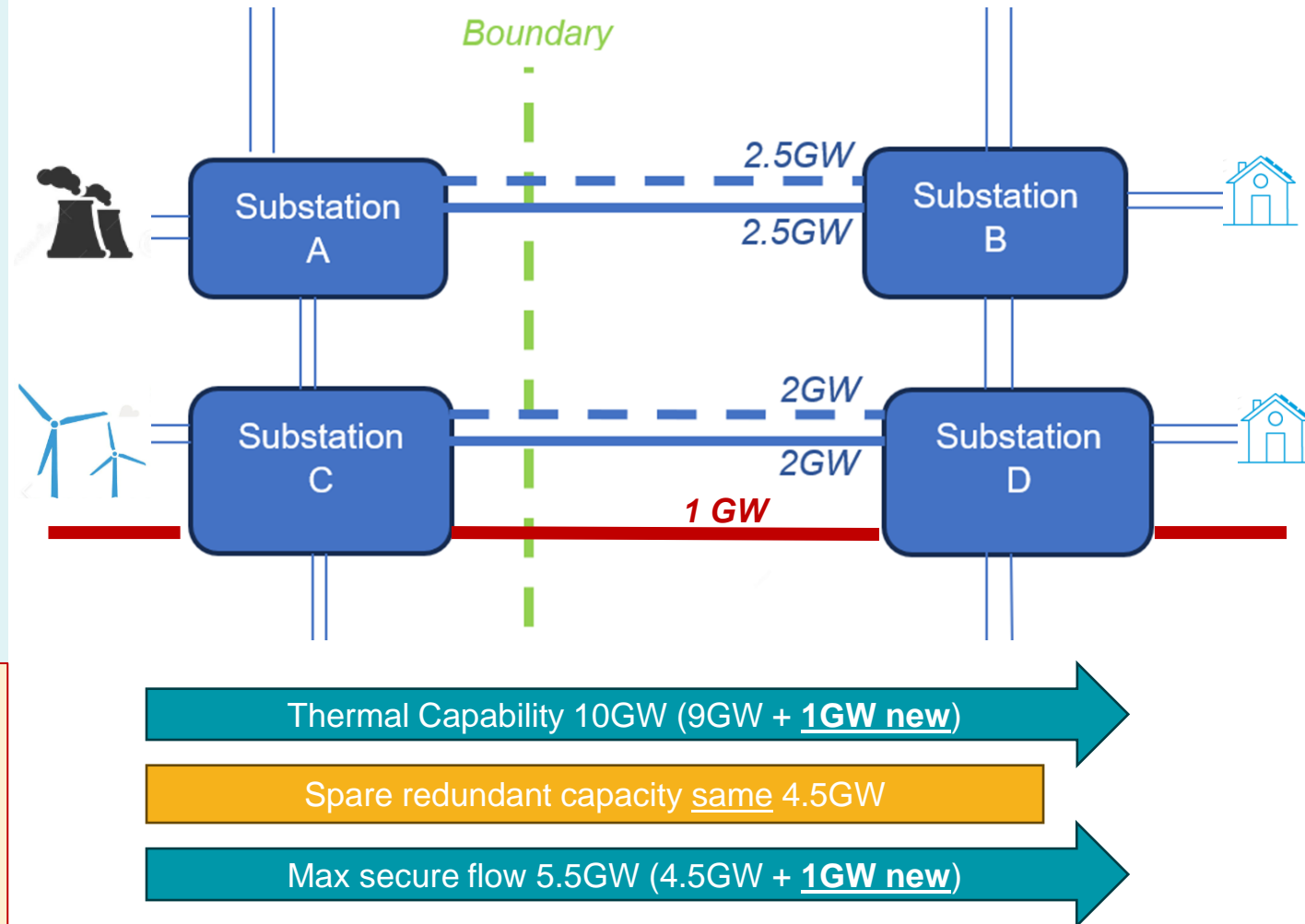
SQSS

TOs plan network additions using SQSS criteria
Surplus capacity is required in case of faults or outages including:

- “N-2” : Outage on two largest separate circuits
- *Worst case fault scenario remains the same*
- *Boundary is still secure*

An additional 1GW of network capacity is required for new generation

- *Build a new 1 GW circuit*
- *Boundary remains secure under SQSS*



What is the issue?

TNUoS says: Want 1GW, build 1.76GW

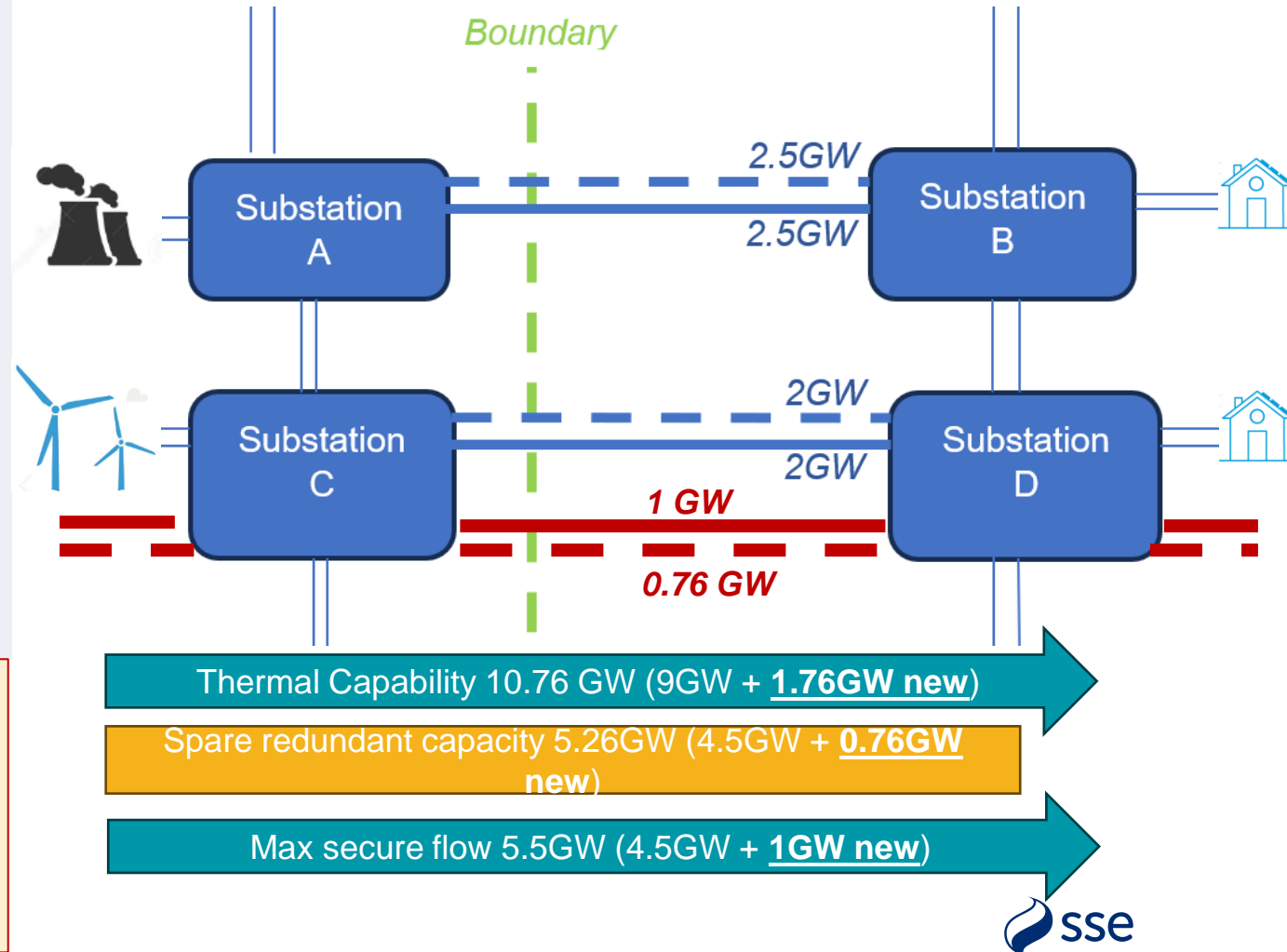
TNUoS

Transport and Tariff model assumes security is a ratio:

- For each 1MWkm of new network, 1.76x this capacity is developed
- Boundary security modelled to increase pro-rata
- $2.5\text{GW} + 2\text{GW} + 0.76\text{GW} = 5.26\text{GW}$ spare capacity

An additional 1GW of network capacity is required

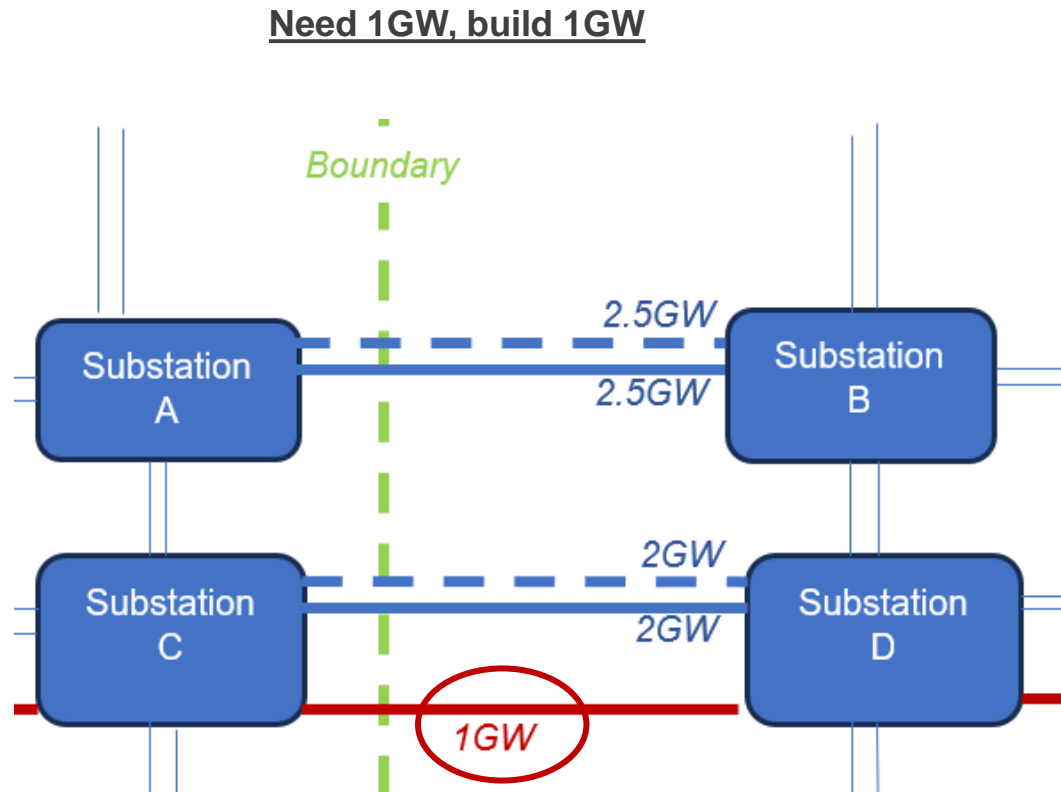
- Build 1.76 GW of network under CUSC methodology
- Boundary is over-secure under SQSS



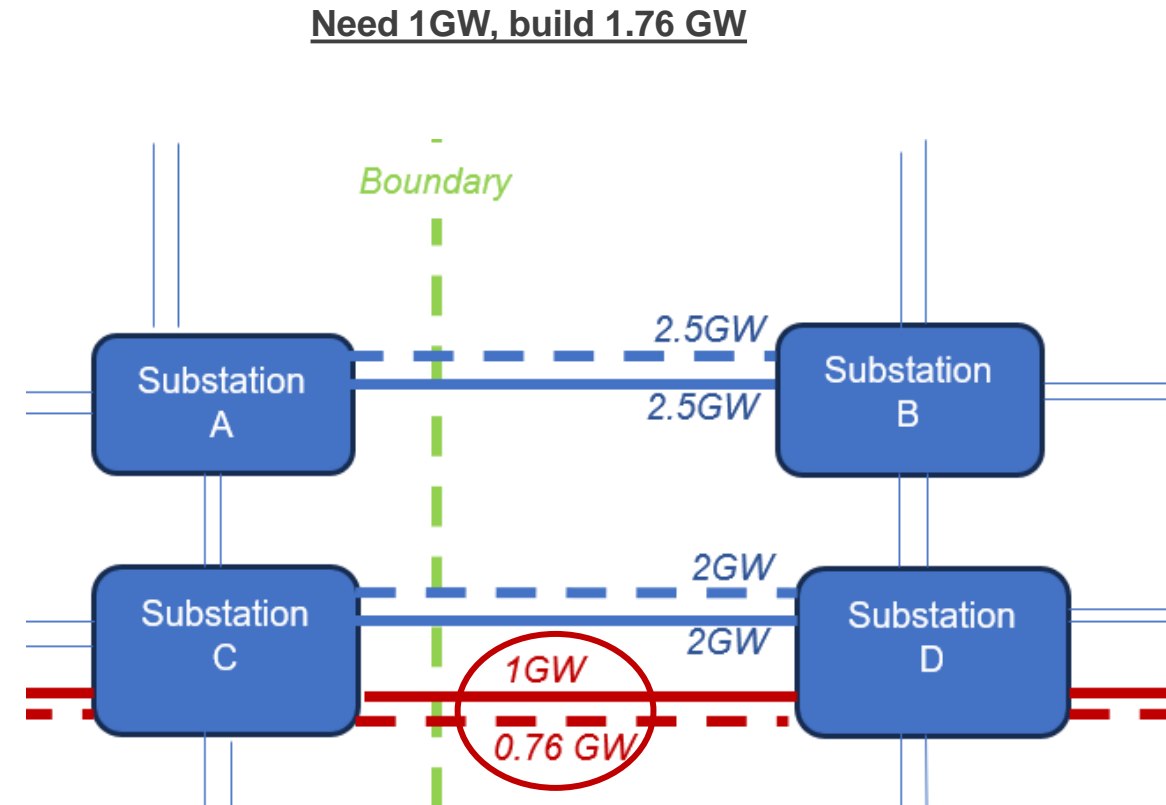
What is the issue?

A difference between how networks are planned vs how the TNUoS model reflects this

TOs plan network additions using SQSS criteria



TNUoS model assumes redundancy is a ratio



TNUoS Transport model is over-forecasting how much redundant network will be planned for security

What is the issue?

A difference between how networks are planned & how the TNUoS model forecasts this

Required redundant surplus capacity is an absolute number in MW

If current MITS boundary is already secure, new circuits don't cause need for additional redundancy for security

Although if new circuit is larger than previous worst case fault, then some additional security measures may be needed

TNUoS charging model applies the Security Factor as a multiplier to all new circuits

For every new circuit, an additional 1.76 times that is assumed to be required and built

Note: Some circuits only have a factor of 1 applied, for example some remote island links and some local circuits

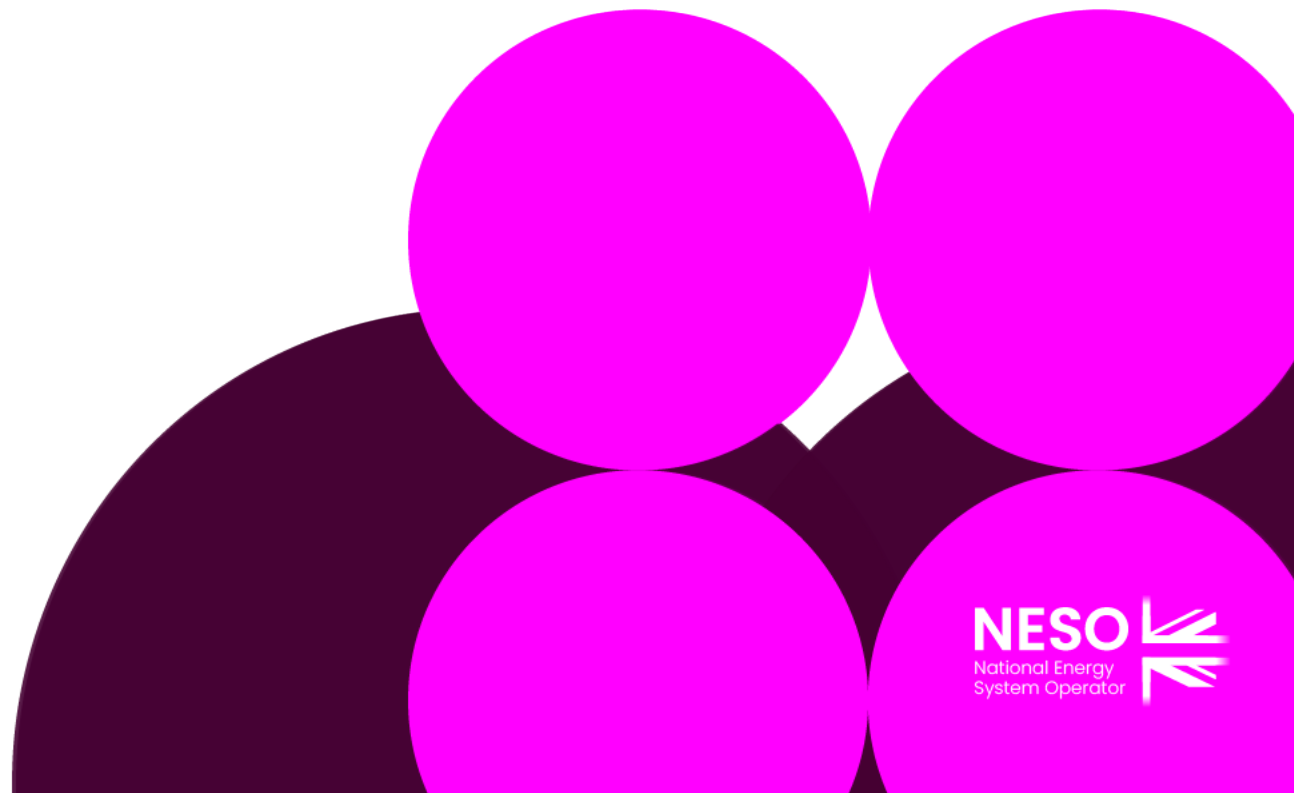
- **Issue:** TNUoS Security Factor for Wider charges is not cost reflective of network planning
- **Solution:** TNUoS Transport model treatment of incremental redundancy should be more cost reflective

Agree Terms of Reference

Sarah Williams - NESO Code
Administrator

Cross Code Impacts

Sarah Williams - NESO Code
Administrator



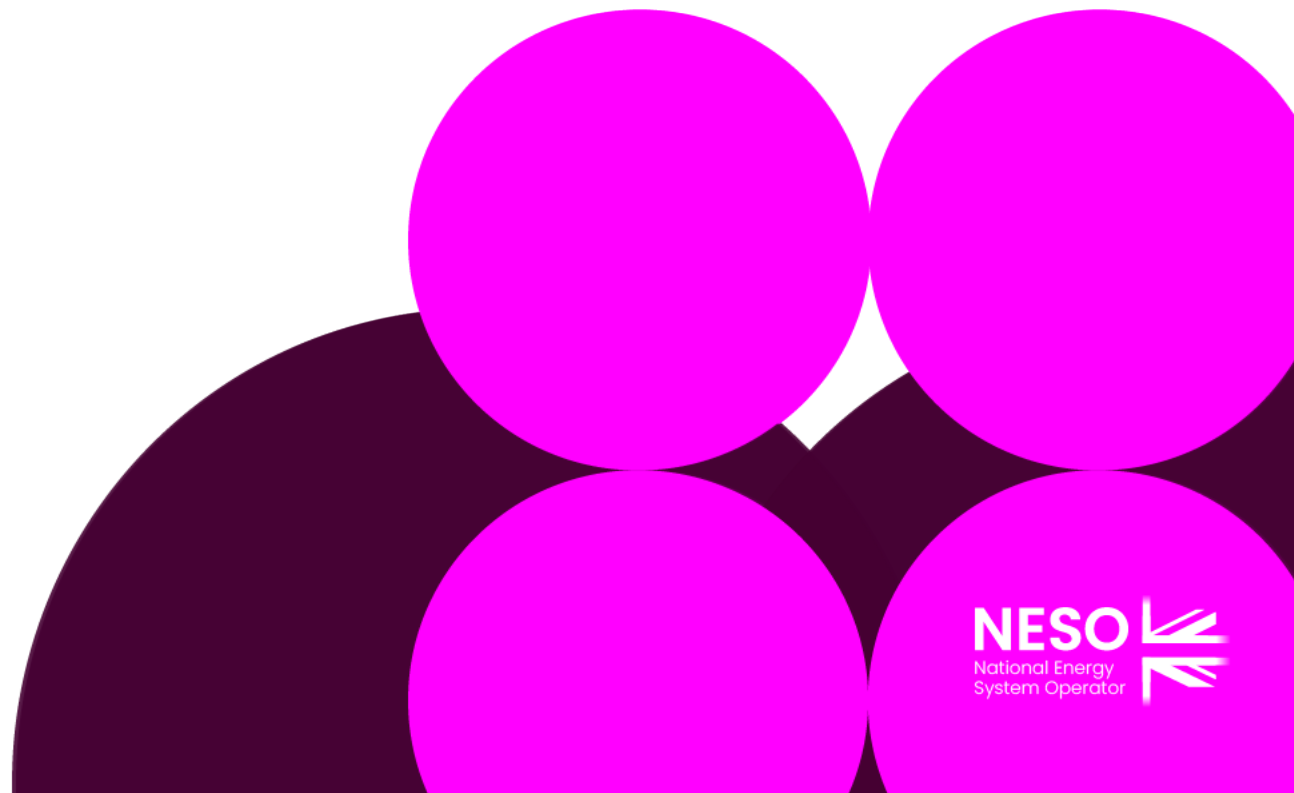
Cross Code Impacts

[CMP444 - Introducing a cap and floor to wider generation TNUoS charges](#)

This modification seeks to introduce a temporary cap and floor mechanism to wider generation TNUoS (Transmission Network Use of System) charges, to reduce investment uncertainty for generators and developers.

Any Other Business

Sarah Williams – NESO Code
Administrator



Next Steps

Sarah Williams – NESO Code Administrator

