
**Supporting document
for the provisional Electricity Cybersecurity
Impact Index (ECII)**

Table of Contents

Introduction.....	3
Legal status of this document.....	3
Provisional ECII for developing the provisional list of high- and critical-impact entities.....	4
Using the provisional ECII for identifying high- and critical-impact processes within an entity	5
High-impact and critical-impact thresholds	6
Setting the thresholds based on reserves	6
Calculating the high-impact threshold	6
Calculating the critical-impact threshold	7

1 Introduction

Under the Network Code for Cybersecurity (NCCS), European Network of Transmission System Operators for Electricity (ENTSO-E) in cooperation with the EU DSO Entity (DSO Entity) has developed provisional Electricity Cybersecurity Impact Indices (ECII) and high- and critical-impact thresholds. This supporting document has been developed jointly by ENTSO-E and the DSO Entity to accompany the provisional ECII and thresholds. It provides all interested parties with information about the rationale for them.

1.1 Legal status of this document

This document accompanies the provisional ECII and is provided for information purposes only. Consequently, this document is not legally binding.

2 Provisional ECII for developing the provisional list of high- and critical-impact entities

This section provides provisional ECII that competent authorities shall use when they develop a provisional list of high-impact and critical-impact entities according to Article 48(3) of the NCCS regulation.

The provisional ECII aim at measuring the possible impact of an entity to the electricity system based on how much load or generation they control. Different definitions are however needed to measure the load and generation for different types of entities.

No provisional ECII are defined for managed security service providers and the DSO Entity, because no provisional high-impact and critical-impact processes have been identified for these entities.

No provisional ECII are defined for ENTSO-E and the Regional Coordination Centres (RCCs) as a detailed analysis of their processes will be needed to determine if they should be on the provisional list of high- or critical-impact entities. Using the maximum total load or maximum aggregated generation output of all the affiliated TSOs as ECII, would likely overestimate the impact of ENTSO for electricity and the RCCs. The processes at these entities would likely only affect a fraction of the load or generation at TSOs. Hence, it is recommended that ENTSO for electricity and the RCCs attempt to directly assess the consequences of cyber-attacks using the impact metrics in the risk assessment methodologies.

The category of electricity undertakings listed in Article 2(1) of the NCCS legal text has been split into producers, transmissions system operators, distribution system operators, and aggregators, as these entity types need different ECII.

3 Using the provisional ECII for identifying high- and critical-impact processes within an entity

This section explains how high- and critical-impact entities can use the provisional ECII to determine which of their internal processes would be considered high- or critical-impact. Entities need to classify their processes to determine which of them could fall under the NCCS.

For processes, entities should use the same ECII as competent authorities to determine the high- and critical-impact entities. While the competent authorities use the ECII to measure the total power controlled by the entity, entities should only consider that part of the ECII that can be controlled through the process.

For certain processes at TSOs, the ECII, based on power controlled, may not be sufficient, as cyber-attacks on TSOs can affect the operational security of the electricity systems in other, more direct ways. Hence, for some processes it is recommended that TSOs directly use the impact metrics in the NCCS risk assessment methodologies. It is expected that a TSO can directly calculate these more advanced metrics, as they are already applying them in the ENTSO-E incident classification scale.

Based on the experiences gained by using the impact metrics directly, more refined ECII may be developed for TSOs during the Union-wide risk assessment.

4 High-impact and critical-impact thresholds

The high-impact and critical-impact thresholds have been based on the minimum dimensions of reserves that TSOs kept. These dimensions have been estimated using publicly available data.

4.1 Setting the thresholds based on reserves

The idea is to base the thresholds on the dimension of the frequency reserves that TSOs keep:

- The **high-impact threshold** should be the minimum size of the frequency restoration reserves (FRR) in a member state.
- The **critical-impact threshold** should be the minimum size frequency containment reserves (FCR) in the synchronous area.

The rationale for setting the thresholds based on frequency reserves is that:

- if an entity can control more power than the FCR, a cybersecurity incident at the entity can cause an imbalance larger than the FCR available to counter it. Such an incident could cause major problems for the whole synchronous area, and hence cause a critical disruption of cross-border electricity flows;
- if an entity controls more power than the FRR but less than the FCR, incidents at the entity will not cause problems in the synchronous area. There are enough reserves to mitigate changes in frequency. However, the country in which the entity is located does not have enough reserves itself to restore the imbalance and the resulting frequency deviation. So, the cybersecurity incident has cross-border consequences in that TSOs in neighbouring countries will be asked to support in mitigating it.

The FRR and FCR thresholds are dimensioned based on reference incidents (see Article 157(2)(d) and Article 153(2) of the System Operations Guidelines). The high-impact and critical-impact thresholds hence would also be close to the size of these reference incident.

Each TSO is required to take measures to be able to handle the reference incident used to dimension the FRR. So, if the consequences of a cyber-attack are below the high-impact threshold, the TSO should be able to counter them with the reserves and measures they have without serious disruptions to the electricity system.

The TSOs in a synchronous area are required to take measures to handle the reference incident use to dimension the FCR. So, if the consequences of a cyber-attack are above the high-impact but below the critical-impact threshold, the synchronous area should be able to counter them. There will be effects on cross-border flows. But the synchronous area will not be significantly disrupted.

4.2 Calculating the high-impact threshold

To determine the minimum size of the high-impact threshold, data is needed on minimum size of the FRR. To ensure that no sensitive information about grid resilience is leaked through the threshold, the NCCS working group decided to base the thresholds on publicly available information whenever possible.

Two data sources from the ENTSO-E transparency platform were used to estimate the minimum FRR:

1. the preferred data source was the Outlook of the reserve capacities on FRR that TSOs share with ENTSO-E for publication under Article 188(3) of the System Operations Guidelines. If this data source was not available on the transparency platform, the TSO was asked to provide it directly;
2. if no FRR outlook was available for a member state, the size of the largest generating unit in the member state was used. According to Article 157(2)(d), the reference incident is the largest imbalance that may result from an instantaneous change of active power of a single power

generating module, single demand facility, or single HVDC interconnector or from a tripping of an AC line within the LFC block. So, we know that the reference incident is at least larger than the size of the largest generating unit.

The size of the reference incidents may be different for reduction of generation (“up”) and loss of load (“down”). To calculate the thresholds, the minimum size of load and of generation was taken. One threshold is used for all entities whether they control load or generation (or both), because in most cases entities can cause incidents both in the up and down direction. For example, an operator of recharging points can cause an incident in the down direction if the recharging points that are in use are suddenly switched off. But it can also cause an incident in the up direction if the recharging points are switched on again.

To simplify the thresholds and ensure they do not change too frequently, the estimates above were rounded off as follows to determine the high-impact thresholds:

Range for the reference incident proxy	High-impact threshold
< 500 MW	250 MW
500 – 1,000 MW	500 MW
1,000 – 1,500 MW	1,000 MW
> 1,500 MW	1,500 MW

The table in the Annex shows the calculation of the thresholds for all member states.

The same high-impact threshold of 1,500 MW is used for Luxembourg as for Germany. The reason is that, in Luxembourg, Creos has delegated the load-frequency control processes to Amprion and is part of their control zone. They are hence using Amprion’s FRR. Note that the peak load of Luxembourg is well below this high-impact threshold.

4.3 Calculating the critical-impact threshold

To determine the minimum size of the critical-impact threshold, data is needed on minimum size of the FCR. For this purpose, the Scale 2 thresholds for incidents on power generating facilities in the ENTSO-E Incident Classification was used.

For isolated systems, the ICS uses the capacity of the power plant with the largest unit in the system. For Cyprus, the threshold was hence based on the Vasilikos Power Station (868 MW), rounded down to 800 MW. For Malta, the threshold was based on the largest unit in the Delimara Power Station (215 MW for phase 4), rounded up to 250 MW.