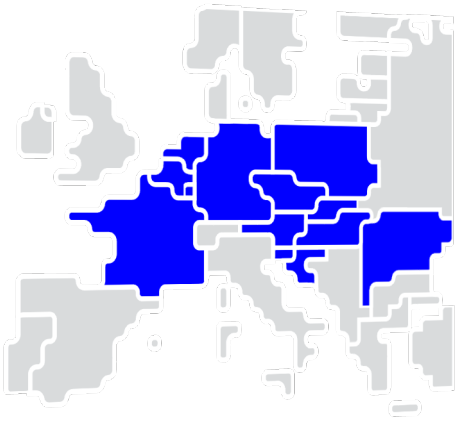


Explanatory document to the Central Europe Capacity Calculation Region methodology for common provisions for regional operational security coordination in accordance with Article 76 of Commission Regulation (EU) 2017/1485 of 2 August 2017

"Explanatory Note"

20th November 2026



Disclaimer:
This document is released on behalf of the transmission system operators ("TSOs") of the Capacity Calculation Region Central Europe solely for the purpose of providing additional information on the methodology for common provisions for regional operational security coordination in accordance with Article 76 of Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on system operations guideline ("SO Regulation").

Table of Contents

Introduction 5
1. General Provisions 6
1.1 Constraints 6
2. Regional Operational Security Coordination 7
3. Definition and determination of CE XNEs, XRAs, constraints and contingencies 8
3.1 XNEs and scanned elements 8
3.2 Classification of remedial actions 12
3.3 Cross-border relevance of remedial actions 13
3.3.1 Qualitative assessment of XRAs 13
3.3.2 Quantitative assessment of XRAs 14
3.4 Contingency list 17
4. Coordinated regional operational security analysis process 17
4.1 Preparation 17
4.2 Coordination 18
4.2.1. General provisions of coordination process 18
4.2.2. Power flow and security analysis 19
4.2.3. Optimisation of remedial actions 19
4.2.4. Time coupled optimisation 21
4.2.5. Relieving operational security limit violations with balanced RAs 22
4.2.6. Avoid additional violations of operational security limits on XNEs and scanned elements 22
4.2.7. Minimise incurred costs 23
4.2.8. RA effectivity 23
4.2.9. Robustness 23
4.2.10 Coordination of XRAs 24
4.2.11. Inter-CCR coordination 25
4.3 Validation 26
4.3.1. Outcome of validation 26
4.4. Implementation of remedial actions 26
4.4.1. Ordering and Activation of remedial actions 26
4.4.2. Consideration of remedial actions in next IGM 27
4.4.3. Fast activation process 27
5. implementation 28
5.1. Monitoring 28
5.2 Implementation 28
6. Allocation of tasks by RCCs 31

6.1 Appointment of RCCs and delegation of tasks to RCCs 31
6.2 Allocation of tasks between RCCs 31
6.3 Assessment of the effectiveness and efficiency 33
6.4 Decision-making process and governance 33

INTRODUCTION

In accordance with Article 76 of Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on system operations (hereafter referred to as the “SO Regulation”) the Central Europe Transmission System Operators (hereafter referred to as “CE TSOs”) submitted the Common Methodology for Regional Operational Security Coordination for the Central Europe Capacity Calculation Region (hereafter referred to as “CE CCR”) to Central Europe NRAs. This methodology aims at the day-ahead and intraday regional operational security coordination within the CE CCR.

The aim of this explanatory note is to provide additional information with regard to the Methodology for Regional Operational Security Coordination for the CE CCR (hereafter referred to as “CE ROSC Methodology”). In particular, it provides insight on the whole process chain defined in CE ROSC Methodology, from the preparation of input data to the optimisation and implementation of cross-border relevant Remedial Actions (XRAs). This paper considers the main elements of the relevant legal framework (i.e. SO Regulation, CACM Regulation and EB guideline),and is provided to gain additional insight on the methodology only.

1. GENERAL PROVISIONS

1.1 Constraints

Different kinds of constraints are mentioned in the CE ROSC Methodology.

Operational security constraints are most commonly current, short-circuit, voltage or stability constraints.
The CE ROSC process shall detect if current limits in N-situation or after occurrence of a contingency are violated. If this is the case, there is a need to prepare and activate a remedial action in order to respect those current limits.

- Constraints on remedial actions: Constraints related to all aspects required to be taken into account when using RAs in accordance with article 20(1) SO Regulation and classified as following:
    - Technical constraints are all the rules that a power source has to comply with for technical reasons such as preparation period, ramping period, full activation time, minimum and maximum power output, deactivation period, minimum and maximum duration of delivery period, limit values for voltage, current or power, etc. As consequence, for Redispatching & Countertrading, at least the following technical constraints are considered:
        i. Minimum and maximum redispatch values (MW)
        ii. Maximum power increase and decrease gradient (MW/h)
        iii. Minimum up and down time
        iv. Lead and Lag time
        v. Start-up and Shut down allowed
        vi. constraints for storage
        vii. Conditional availability depending on activation of another RA
    - Operational constraints means all the operational conditions and usage rules taking into account the timings to operate the grid (for example, an operator can only activate a limited number of remedial actions in a given period) and avoid a premature use of the network elements (limitation of the frequency of switching of one breaker, synchronized change of PST taps).
    - Procedural constraints mean all the timing constraints due to local or regional processes e.g.:
        i. timings T0 to T5 according to article 45 CSAM to be respected during DA CROSA;
        ii. Maximal time to perform the remedial actions optimisation
        iii. time to perform a local security analysis
        iv. Timings to request a Remedial Action from a non-CE TSO, etc.
    - Legal constraints mean the legal requirements stated in national laws such as the priority of activation of remedial actions. For example, some countries can legally not downregulate RES even though it is less expensive or more efficient to solve a given flow constraint.

- For the detection of other constraints, such as voltage violations, violations of short-circuit current limits or violations of stability limits, each CE TSO should perform local assessment and long-term operational security analysis in accordance with articles 31, 38 and 73 of SO Regulation. TSOs will deal with these constraints, thanks to the definition of system constraints or/and local security assessment. System Constraints are additional optimisation constraints added by TSOs, expressed as flow limitation on one or a sum of Secured and/or Scanned elements and necessary to

substitutional respect stability limits or operational security limits other than current limits. For example, to prevent stability violations, a TSO could limit the overall amount of power flow on three network elements (for example 1000 MW) even though the sum of the capacity of these three elements is above 1000 MW. TSOs specifying such or other system constraints shall share transparently with CE RCCs and TSOs the information justifying their application.

2. REGIONAL OPERATIONAL SECURITY COORDINATION

As illustrated in figure 1, the CE Regional Operational Security Coordination (ROSC), that shall be executed for each hour of the target day, is composed of the following activities:

- One day ahead Coordinated Regional Operational Security Assessment (DA CROSA) in day ahead timeframe (hereafter referred to as 'DA CROSA')
- A minimum of three Intraday Coordinated Regional Operational Security Assessment (hereafter referred to as 'ID CROSA') in the Intraday timeframe

- CROSAs shall be performed in accordance with article 23 and 24 of CSAM.
- Each CROSA shall consist of:
  i. Preparation phase;
  ii. Coordination phase;
  iii. Validation phase.
- The implementation of the Agreed Remedial Actions (RAs) in the subsequent individual grid models (IGMs) and activation of the Ordered RAs.
- Modification of an Ordered RA or activation of a new RA might be considered following the fast activation process.

The different steps of the DA CROSA process will be performed respecting the timings T0 till T5 defined in accordance with the Methodology for coordinating operational security analysis in accordance with article 75 of SO Regulation (hereafter referred to as 'CSAM').

A minimum of three ID CROSA shall be performed considering the three mandatory CGMs which have to be built for 00h00, 08h00 and 16h00 according to CGMM.

More details about the preparation and coordination phases are given in the relevant chapters of this Explanatory Note.
The validation phase shall mainly consist of the formalization, communication, reporting and archiving of the CROSA results. In DA, in line with the Methodology for coordinating operational security analysis in accordance with article 75 of SO Regulation (hereafter referred to as 'CSAM'), this formalization shall take place through a pan-European conference with representatives of all RCCs and TSOs.

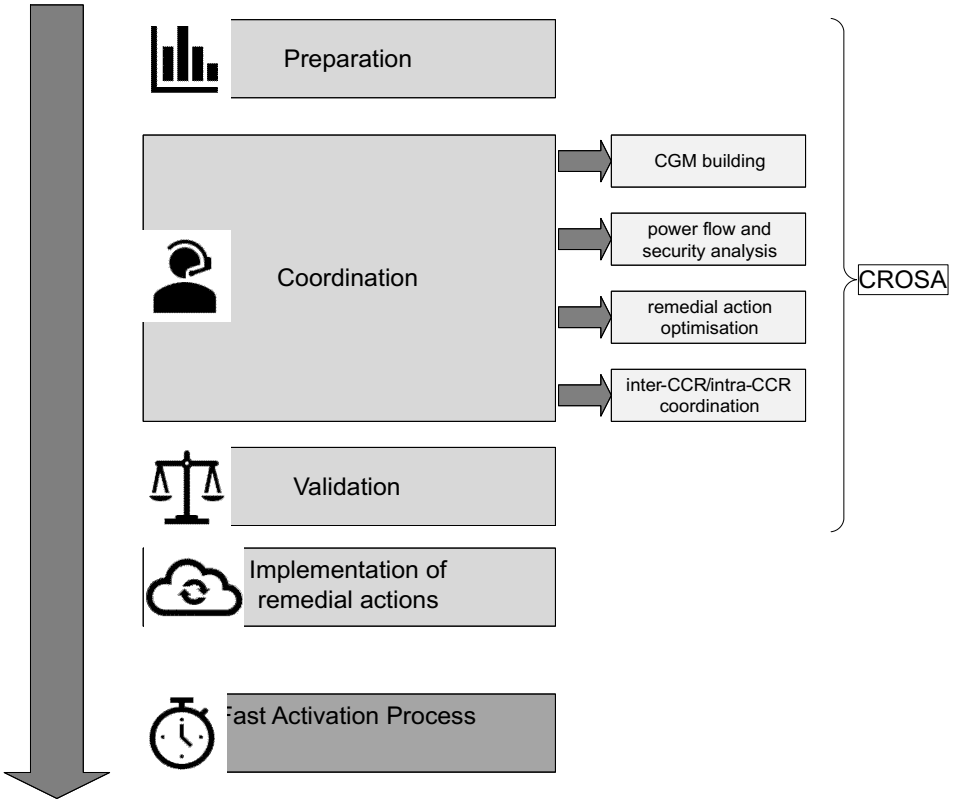


Figure 1: Overview Coordinated Regional Operational Security Assessment (CROSA) process

On top of the ROSC process, CE TSOs with CE RCCs shall perform intraday regional security analysis ('ID RSA'). The goal of the ID RSA is to provide CE TSOs each hour of the day with the latest information about the loading of the grid and previously undetected violations of operational security limits, which may serve as a trigger for a fast activation process.

3. DEFINITION AND DETERMINATION OF CE XNES, XRAS, CONSTRAINTS AND CONTINGENCIES

According to article 15 of CSAM, *cross-border relevant network elements (XNEs) shall be all critical network elements ('CNEs') and other network elements above the voltage level defined by TSOs, except for those elements for which all TSOs in a CCR agree that they are not cross-border relevant for the concerned CCR and may therefore be excluded*.

3.1 XNEs and scanned elements

In order to harmonize definitions used across CCRs and to use same terminology in future processes, ENTSO-E proposed to define and use the following wording in all regional ROSC methodologies:

- A **XNE, as defined in the CSAM,** is an assessed element on which, when violations of an operational security limit are identified during the regional or cross-regional security analysis, remedial actions needed to relieve these violations shall be identified.
- A **Scanned element** is an assessed element on which the electrical state (at least flows) may be computed and may be subject to an observation rule during the regional security analysis process. Such observation rule can be for example to avoid increasing a constraint or to avoid creating a constraint on this element, as a result of the design of the remedial actions needed to relieve violations on the secured elements.

CE TSOs include network elements in their IGMs in line with the CGMM and CSAM, which include network elements of different voltage levels (including <220 kV). Most relevant network elements for the CROSA process to be defined as XNEs are the network elements on 220 kV and 380 kV level, as these elements are used to facilitate the energy exchanges between bidding zones within the European energy system. Yet, it has to be noted that in some countries the grid of a voltage level lower than 220kV is not operated by the TSOs but by distribution system operators. Although in accordance with Article 6 of CGMM, grid elements of a voltage level lower than 220 kV may be included in the grid model, this does not mean that TSOs have to actively relieve congestions in these grids during the CROSA. It is rather meant to ensure that a RA used for the High Voltage grid will not lead to (further) congestions in the lower voltage grids. The impact of these lower voltage grids also has to be determined on the 220 and 380 kV grids. This will be achieved by introducing scanned elements into the ROSC methodology.
In contrast, considering only elements with a voltage level equal or higher than 380kV as XNEs, would mean that 220kV elements which have cross-border relevance would not be considered in the regional or cross-regional process. Having this in mind, CE TSOs decided to consider all elements with voltage level equal or higher than 220kV as XNEs (CE XNEs) and decided to define criteria for which certain elements can be discarded as XNE.

If one of the following criteria is fulfilled, CE TSOs shall have the right to exclude elements from the list of XNEs without prior agreement by other TSOs:

- Element is a power plant line: e.g. line connecting a substation to which only generation is connected to the meshed grid and is therefore not relevant for CROSA processes.
- Element is a radial line: e.g. elements operated in radial topology; connected to a substation that is not connected to any other substation at a voltage level higher or equal than 220kV.
- Element is connected to a DSO grid: e.g. elements operated by DSOs at a voltage level equal or higher than 220kV that have distribution character.
- Element is a transformer with the secondary voltage side lower than 220kV e.g. transformers connected to DSO grids.

The following figure 2 shows which elements (highlighted in yellow) can be discarded from the list of XNEs in accordance with the provisions explained above.

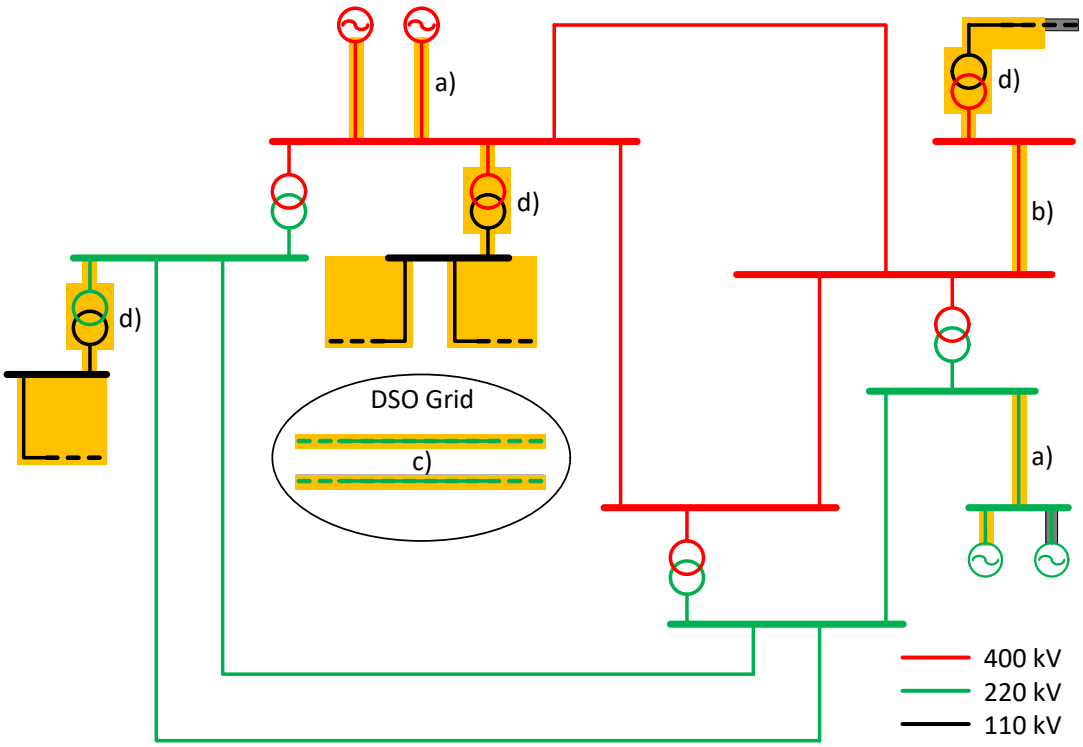


Figure 2: Elements (highlighted in yellow) which can be discarded from the set of CE XNEsIn addition to these criteria, any element can be discarded from the list of XNEs , when a common agreement among CE TSOs is reached. This could be the case, if a part of the grid is almost not influenced trans-regionally. However, such a rule cannot be applied to the Critical Network Elements in accordance with Article 5 of day-ahead and intraday capacity calculation methodology of the CE CCR.

The common agreement among Central Europe TSOs shall mean the unanimous agreement of all Central Europe TSOs. For the purposes of reaching such common agreement, a deemed acceptance approach shall apply, whereby the absence of an explicit objection within the applicable coordination timelines shall be considered as acceptance. A Central Europe TSO objecting to a proposal shall make reasonable efforts to clearly state and substantiate the reasons for its objection in a timely manner.

TSOs which are part of more than one CCR shall have the right to discard any of their elements from the list of XNEs which are regarded as XNE in another CCR without prior agreement by other TSOs. In such case, the concerned TSO shall have to inform the other TSOs and RCCsAs suggested by ENTSO-E, CE TSOs define scanned elements as list of elements on which the CROSA shall not create new operational security limits violations or worsen any existing violation, except if agreed pursuing Art. 23 (2). Such elements can be elements which are discarded from the list of XNEs with voltage level lower than 220kV. In the latter case, these elements have to be included in the IGM and TSOs shall provide justification of their inclusion in the set of scanned elements (e.g. elements influenced by RA used to solve constraints on XNEs). Such an inclusion must be compliant with the CGMM.

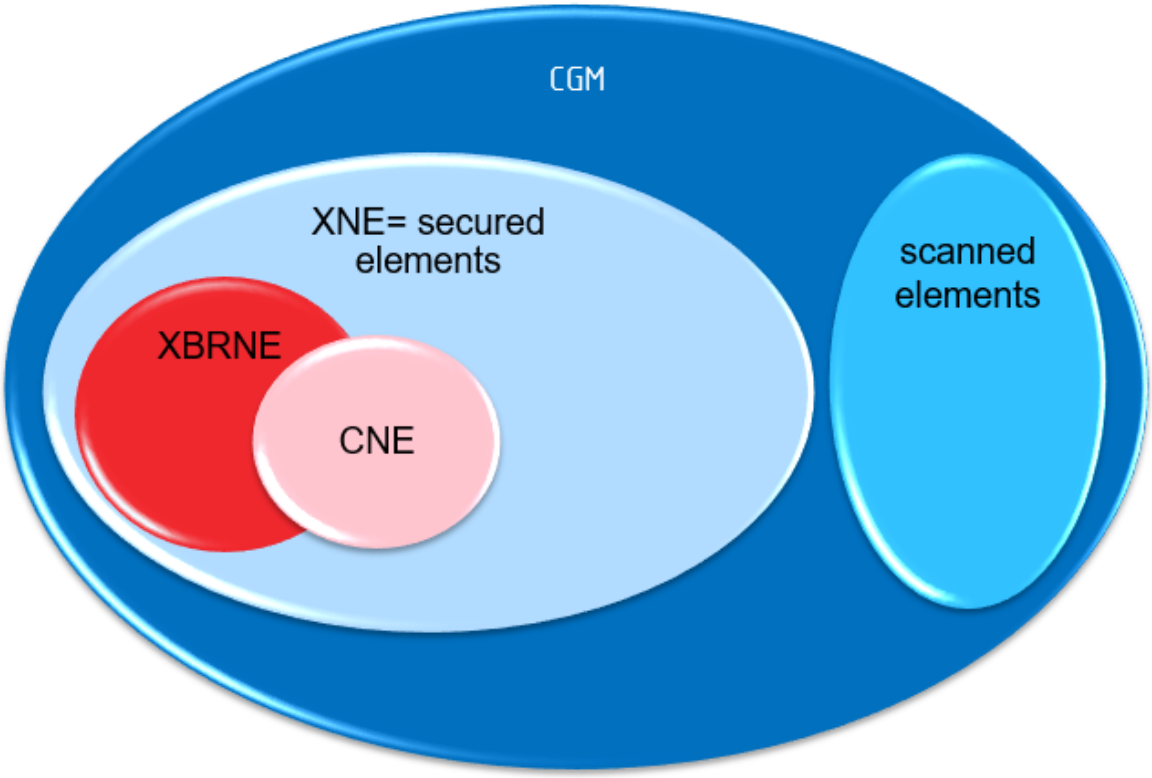


Figure 3: secured and scanned elements

CE TSOs shall have the right to update the lists of XNEs and scanned elements at any time (e.g. due to commissioning of a new element or seasonal changes) considering that:

- Any element with a voltage level equal or higher than 220kV is regarded as XNE by default and therefore any new element at such a voltage level can be included in this list of XNEs.
- Discarding an element from the list of XNEs is subject to common agreement by CE TSOs as defined earlier in this chapter, except for those elements, that fulfil one of the criteria defined in this chapter.
- Any discarded element from the list of XNEs can be included in the list of scanned elements, but it is not mandatory.
- Each CE TSO shall have the right to move any elements it operates with a voltage level equal or higher than 220kV from the list of scanned elements to the list of XNEs.
- Each TSO shall have the right to include any new element with a voltage level lower than 220kV in the list of scanned elements. Such elements have to be modelled in IGM.

CE TSOs shall have the right at any time to exclude any element from the list of scanned elements. CE TSOs shall update the list of XNEs and the list of scanned elements lwhen necessary and inform the RCC about the change.

First lists of XNEs and Scanned Elements shall be established by TSOs with the support of RCCs 12 months before the implementation of the first step of the methodology
Both lists shall be reassessed by each CE TSO at least once a year.

Lists of XNEs and scanned elements will be made available before each CROSA process.
Each CE TSO shall have the right to set individual thresholds for overloads for the scanned elements (e.g. 110kV line), for CROSA purposes only, reflecting the fact that TSOs are able to accept certain overloads on such elements. This could be the case, if there are for example additional RAs not explicitly modelled in the CGM, which can further relieve the violation on the scanned element.

3.2 Classification of remedial actions

Each CE TSO has to prepare a list of remedial actions which can be used to relieve at least violations of the CE TSO's current limits. CE TSOs shall design these RAs taking into account the categories defined in article 22 of the SO Regulation but not limited to them.
Within one month, after the set of secured elements has been defined, CE TSOs shall share with CE RCCs all potential RAs.

In accordance with article 14(2) of CSAM, a RA can be designed as a single action or a combination (set) of actions as listed in article 22 of the SO Regulation. If a RA consists of multiple actions, it still should be treated as one. One example of such RA can be a simultaneous change of scheduled exchanges on at least two HVDC links of the same amount of power in opposite directions (rescheduling of DC flows).

When designing a RA, CE TSOs have to include all the relevant information such as availability timeframe, activation time, costs (for costly RAs) and all constraints limiting its usage. In accordance with article 16 of CSAM for each RA shall be identified its cross-border relevance. How to identify the cross-border relevant remedial actions has been introduced in Articles 10, 11 and 13 of this Methodology.

RAs have different statuses depending on their availability and the progress in the process. Available RAs are RAs that are technically feasible and can be considered for relieving operational security violations, while a conditionally available RAs can only be used when predefined conditions related to system conditions, operational constraints or other limitations are fulfilled.
Based on the RAO outcomes, the optimal RAs are determined and are recommended by the RCCs to the TSOs. Such recommended RAs become agreed RAs once they are agreed or agreed with modifications during the coordination process between the TSOs and RCCs.

Agreed RAs becomes ordered RAs when the TSOs determine that its activation cannot be postponed until the next CROSA due to specific activation constraints, such as the required activation time.
Activated RAs are ordered RAs that have been implemented by the XRA connecting TSOs, or for which the request for activation has been sent to the relevant resource provider. Therefore, the RA status progression reflects the transition from the availability of an RA, through its recommendation and coordination, towards its ordering and final activation.

3.3 Cross-border relevance of remedial actions

In accordance with the CSA methodology, all potential remedial actions (RAs) are presumed to be cross-border relevant (XRAs), unless all CE TSOs unanimously agree that a potential RA is not cross-border relevant. Consequently, the methodology focuses on identifying the TSOs affected by the activation of an XRA rather than on determining whether a remedial action itself is cross-border relevant.

For each XRA, the CE TSOs jointly identify the XRA affected TSOs using a qualitative approach and, where no agreement can be reached, a quantitative assessment in accordance with the methodology. This process determines the TSOs that need to be involved in the coordination of the XRA activation.

Considering the definition of XNEs, some XRAs may only have a significant operational impact within the control area of the connecting TSO and therefore only affect that TSO. In such cases, although the remedial action remains classified as an XRA, its activation during the fast activation process is not subject to further coordination when the connecting TSO is also the only XRA affected TSO. The other CE TSOs and the CE RCC(s) are informed of the activation in accordance with the methodology.

3.3.1 Qualitative assessment of XRAs

CE TSOs shall aim at agreeing on a qualitative approach to determine RAs that are deemed cross-border relevant and to identify corresponding TSOs affected by those RAs. The identification of RA-affected TSOs complements the process for determining cross-border relevant RAs by identifying the TSOs for which a given RA has a significant operational impact. The process is based on individual assessments carried out by the TSOs. Each CE TSO evaluates the impact of the RA on its own control area, while the RA Connecting TSO also assesses its impact on the control areas of the other CE TSOs. Performing these assessments from different perspectives allows the TSOs to compare their conclusions and supports a consistent determination of the TSOs affected by the RA.

The assessment is qualitative and may be supported by operational experience, historical system behaviour, network studies or other technical considerations, depending on the characteristics of the RA. The methodology does not prescribe a specific assessment method, allowing TSOs to use the information and expertise most appropriate for the case under consideration.

Where a CE TSO concludes that an RA has a significant impact on its control area, it shall communicate its assessment to the RA Connecting TSO together with the justification for being considered an RA-affected TSO.

For remedial actions that can be expressed by measurable quantities, the assessment of cross-border relevance should be supported by predefined thresholds. These thresholds indicate the level above which a remedial action is considered to have a potentially significant impact beyond the control area of the connecting TSO and should therefore be treated as cross-border relevant. The applicable thresholds should be defined according to the characteristics of the respective remedial action.
For phase-shifting transformers (PSTs), the threshold may be expressed either as a change in the tap position or as the resulting change in power flow. For redispatching and countertrading, thresholds should be specified for the total respective volumes of active power variation . For HVDC systems, the threshold should be defined as a deviation from the scheduled set point. These thresholds provide a

common basis for the qualitative assessment while ensuring a consistent interpretation of cross-border relevance across the CE TSOs.

Determination of RA-Affected TSOs

The determination process is based on the following principles:

- Each CE TSO shall independently assess the impact of each identified RA on its own control area. The assessment shall consider whether the RA has a significant operational impact on the transmission system operated by that TSO.
- The RA Connecting TSO shall additionally assess the impact of the RA on the control areas of the other CE TSOs as well as on its own control area. This parallel assessment provides a common basis for comparing the views of the TSOs and facilitates a consistent evaluation of the geographical scope of the RA.
- The assessment may rely on operational experience, system knowledge, historical observations, planning studies, expert judgement, or other relevant technical evidence. The methodology does not prescribe a single assessment technique, allowing TSOs to apply the most appropriate approach depending on the characteristics of the RA.
- Where a CE TSO concludes that an RA has a significant impact on its control area, it shall submit a justified request to the RA Connecting TSO to be designated as an RA-affected TSO. The justification should explain the basis for the conclusion and the operational considerations supporting the request.
- The CE TSOs shall exchange the outcomes of their assessments and discuss any differences in their conclusions. Where necessary, additional technical information or operational evidence may be provided to facilitate a common understanding.
- The designation of RA-affected TSOs shall be based on common agreement among the CE TSOs. A TSO shall be designated as an RA-affected TSO where the TSOs collectively agree that the RA has a significant impact on its control area.
- Where no other CE TSO requests to be designated as an RA-affected TSO, the RA Connecting TSO shall be considered the sole RA-affected TSO.

3.3.2 Quantitative assessment of XRAs

In case that CE TSOs cannot agree on a qualitative approach for a certain RA, a quantitative approach as described in article 15 (4) of CSAM shall be used:

“In case of a quantitative approach, the cross-border relevance of remedial actions shall be assessed with the remedial action influence factor. The remedial action influence factor shall be calculated for at least each cross-border relevant network element and each contingency (for example each ‘XNEC’) as a simulated flow deviation on a XNEC resulting from the simulated application of a remedial action normalised by the permanent admissible load of the associated XNE.”

The influence factor is calculated as follows:

$$IF_{RA} = MAX_{\forall s, \forall x \epsilon X, \forall c \epsilon C} \left(\frac{\left| P_{s,RA}^{x,c} - P_{s}^{x,c} \right|}{PATL^{s,x}} \cdot 100 \right)$$

Where
IF_{RA}: Influence factor of a RA on the TSO's control area (in %);
s: Scenarios;
x: XNE connected inside TSO's control area where the active power difference is observed;
X: set of XNEs connected inside TSO's control area for which the assessment is performed
c: Contingency;
C: set of contingencies to be assessed;
$P_{s,RA}^{x,c}$: Active power flow or current through the XNE in scenario s with contingency c and RA applied;
$P_{s}^{x,c}$: Active power flow or current through the XNE in scenario s with contingency c;
$PATL^{s,x}$: Permanently Admissible Transmission Loading is the loading in A (MW or MVA) that can be accepted by XNE in the scenario s for an unlimited duration

If a RA consists of a combination of actions, its cross-border relevance shall be assessed based on the combined effect of all actions included in the RA.. A TSO shall be considered as an XRA affected TSO if the Remedial Action Influence Factor (IFRA), calculated in accordance with the CSAM, is equal to or greater than 5% on at least one XNE for which that TSO is the XNE connecting TSO. Consequently, all CE TSOs meeting this criterion shall be considered as XRA affected TSOs. If the calculated IFRA is below 5% for all such XNEs, the RA shall be considered as non-cross-border relevant. The 5% significance threshold may be changed if agreed by the CE TSOs in accordance with the governance framework defined in Article 36 of the methodology.

TSOs shall delegate relevant steps of the tasks relating to the quantitative assessment to their respective CE RCCs.

- Once the assessment of remedial actions have been performed, the list of cross-border relevant remedial actions together with the affected TSOs will be shared among CE TSOs and will be provided to CE RCCs.
- Reassessment of the list of cross-border relevant RAs shall be done on a yearly basis. Nevertheless, each CE TSO shall have the right to request an additional assessment of a RA providing justification for such a request to the RA Connecting TSO and respective CE RCCs.

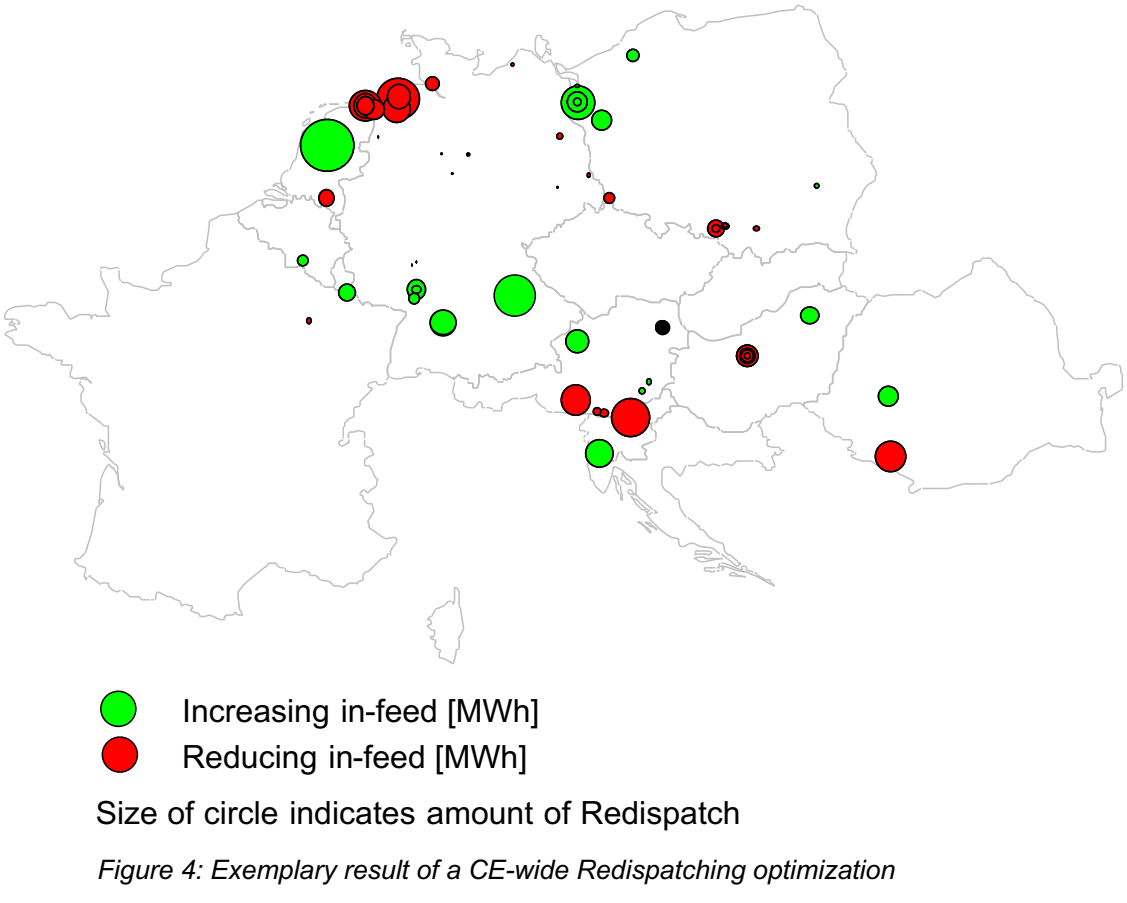


Figure 4: Exemplary result of a CE-wide Redispatching optimization

Additional CE TSOs participating in the CROSA coordination steps are determined via the effect of the overall solution on their respective XNECs. If the influence factor of the combination of RAs proposed by CROSA on a given XNEC, calculated in the same way as for determination of XRAs, is greater than the threshold defined in article 15 (5) of CSAM, then the owning TSO of the XNEC is considered affected.

All CE TSOs which are affected by the global solution or individual XRAs, as well as all RA connecting TSOs participate in the further coordination steps.

The determination of the cross-border relevance of RAs in the process of fast activation is different. Due to the manual nature of this process and in most cases only corrective actions in an existing result, for these measures a clear assignment of individual measures also in terms of redispatching and countertrading can be done. In order to determine the cross-border relevance of these measures, use can be made of the process described in Articles 10-12 of the CE ROSC methodology. The TSOs first determine ex-ante usual RD & CT measures and determine their cross-border relevance for these and all non-costly RAs based on their experience. For RD & CT, the determination for each selected combination could be done per MW, for PSTs per tap position and for topological measures based on their binary state (qualitative approach). The resulting list will be harmonized with all other TSOs in accordance with Article 11 of the CE ROSC. In the case of a lack of agreement, a quantitative determination as in Article 12 of CE ROSC will be applied. If RAs or combinations of RAs are selected in the context of the Fast Activation Process and were not determined ex-ante (e.g. very unusual ones),

it is to be determined by the activating TSO to what extent the measures have an impact on other TSOs by means of appropriate tools based on load flow calculations and coordinate with these TSOs prior to ordering the measures. The task of ad hoc determination of the cross-border relevance of RAs can be transferred to the RCC.

3.4 Contingency list

When performing operational security analyses, each TSO shall, in the N-Situation, simulate each contingency from its "contingency list" and verify that the operational security limits in the (N-1) situation are not exceeded in its control area (Art.72.3 SO GL). Such contingency list, in a highly meshed network, shall include all the internal (inside the TSO's control area) and external (outside TSO's control area) contingencies that can endanger the operational security of the TSO's control area (Art.33 SO GL).

This list should be established based on provisions defined in CSAM (article 10 and related articles). Each CE TSO should prepare a contingency list only with elements relevant for CE CCR and used in CE CROSA process. That means elements located in the TSO's control area which are assigned to different CCR should not be placed on the contingency list provided to CE RCCs unless contingency on that element can endanger the operational security limits on the secured or scanned elements defined in CE CCR.

Such established contingency list should be made available to both CE RCCs and CE TSOs during the preparation phase and should be updated by TSOs when relevant, especially when the conditions are met to apply temporary occurrence increasing factors for exceptional contingencies or when a significant change in the grid occurred. RCCs shall always use the latest Contingency lists shared by the TSOs, which means that it is up to TSOs to decide if they want to send the contingency list for each CSA run or only if there is an update of the list.

The contingency list is maintained under the responsibility of the respective CE TSO and shall reflect the network conditions relevant for the CROSA process. Any proposal to add or remove contingencies, or to modify the set of associated XNECs, should be supported by an appropriate technical justification and communicated to all CE TSOs. Where a proposal concerns the exclusion of XNECs from the assessment of a contingency, the decision shall be taken on the basis of a common agreement among all CE TSOs. To facilitate the maintenance of the contingency list and avoid unnecessary delays, a deemed acceptance process may be applied. Under this approach, a proposal shall be considered accepted if no justified objection is received from the concerned CE TSOs within the agreed review period. Where an objection is raised, the proposal shall be discussed among the concerned TSOs until a common agreement is reached.

4. COORDINATED REGIONAL OPERATIONAL SECURITY ANALYSIS PROCESS

4.1 Preparation

The preparation phase aims at gathering all relevant inputs for the CROSA. Each CE TSO shall make available the following input data to CE RCCs:

- IGMs prepared in accordance with CSAM and the CGMM, including the operational security limits for each XNE and scanned element;
- XNEs and scanned elements;
- The contingency list;
- All available XRAs within the TSO's control area;
- Constraints applicable to XRAs, including technical, operational or procedural limitations;
- System constraints, where relevant;

The input data shall cover all hours for a business day related to intraday and day-ahead CROSA, meaning that:

- In day-ahead input data are provided for the 24 hours of the next business day;
- In intraday, input data are provided for the remaining hours until the end of the same day.

CE TSOs shall deliver or update when required the input data respecting format and process deadlines commonly agreed during the implementation. When providing an update of the list with available RAs, CE TSOs shall re-assess their availability and consider the agreed outcome of previous optimisations in accordance with Article 14 of CE ROSC Methodology.

When receiving any input data, the CE RCC shall perform a quality and consistency check aiming at identifying any format error or any inconsistency with the information contained in the IGMs. The CE RCC shall then report these errors to the CE TSOs to give him the opportunity to correct them prior to the coordination phase.

4.2 Coordination

4.2.1. General provisions of coordination process

The coordination run consists of the following four steps. These steps are further described in the Articles 18 to 28 of the CE ROSC Methodology.

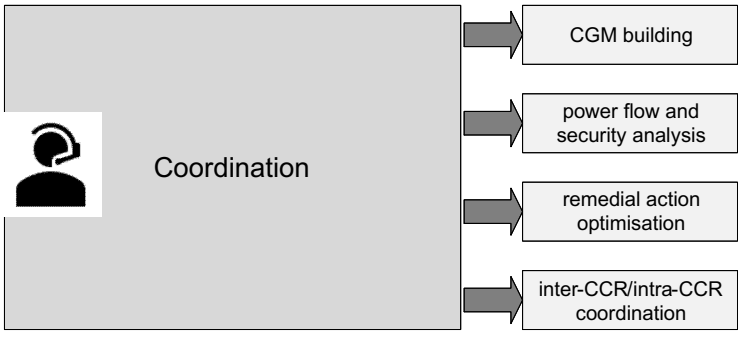


Figure 5: Overview coordination process

The day-ahead CROSA includes two of those coordination runs, which are carried out sequentially. There will be at least three ID CROSAs and each will include at least one coordination run also. Two runs are needed in day-ahead so that the impact of every RA identified during the first run can be

assessed during the 2nd run, not only on lower voltage levels within CE TSOs, but also by the other CCRs and non-CE TSOs.

Intra-CCR coordination describes the coordination between CE TSOs and CE RCCs, while inter-CCR coordination refers to the coordination between CE TSOs and RCCs with the TSOs and RCCs of other CCRs.

4.2.2. Power flow and security analysis

CE RCCs perform the power flow and security analysis on the merged IGMs. For the base case, and each contingency case, an AC load flow is run to identify security limit violations on network elements. CE TSOs have the opportunity to double-check the results of these load-flow calculations, for identifying potential input data errors that would affect the quality of the analysis.

The mitigations of these security limit violations, i.e. the remedial actions, are consequently identified by the consequent process step, the optimization.

4.2.3. Optimisation of remedial actions

An optimization of XRAs has to be done in order to identify in a coordinated way the most effective and economically efficient XRAs. In order to minimise the complexity for the optimization and considering violations of short-circuit current limits, voltage limits and stability limits are more local issues, the described optimization will aim at solving current operational violations while violations of short-circuit current limits, voltage limits and stability limits shall be tackled by TSOs local security assessment as specified in Article 22(4) of the CE ROSC Methodology or by adding further system constraints. The results of the violations of operational security limits resulting from these TSOs local assessments which have impact on the status of available XRAs will be communicated to other CE TSOs and CE RCCs.

Main goal of the optimisation process and part of the CROSA is that each TSO shall maintain currents (or translated power flows) through XNEs within the operational security limits defined when the system is in normal state and after the occurrence of a contingency. These current limits may correspond to PATL and TATL values and may be represented by seasonal limits, dynamic limits or fixed limits depending on the characteristics of the network element.

In accordance with article 21 of the CE ROSC Methodology, the optimisation shall be performed considering all available XRAs and all constraints on XRAs provided by Central Europe TSOs.

In accordance with article 24 of the CE ROSC Methodology, the RAO shall determine the optimal set of XRAs and their volumes while respecting the following objectives, in order of priority:

- relieving operational security violations in accordance with Articles 22 and 23;
- minimising the total sum of costs and revenues of XRAs;
- minimising the amount and volume of activated XRAs.

If no feasible solution can be found, the RAO may relax these objectives to the minimum extent required and in reverse order of priority. The optimization should be able to identify XRAs relevant for congestion management among the categories of remedial actions as described in Article 22 of SO Guideline but not limiting to them. To facilitate the implementation of the optimization solution, the following RAs shall be taken into account:

- actively impact power flows by means of:
    i. tap changes of the power transformers;
    ii. tap changes of the phase-shifting transformers (PSTs);
    iii. modifying topologies;
- redispatch transmission or distribution-connected system users within the TSO's control area, between two or more TSOs;
- countertrade between two or more bidding zones;
- adjust active power flows through HVDC systems;
- modify the duration of a planned outage or return to service transmission system elements to achieve the operational availability of those transmission system elements.

When optimizing RAs, technical constraints shall be considered. For example, for topological RAs (including PST), TSOs consider a maximum number of preventive topological actions per TSO between successive hours (either by taking into account a maximum number X of preventive topological actions per TSO between successive hours. The value X depends on each TSO operational constraints or by progressively penalizing the number of actions above a threshold Y.

In order to avoid damage or too high impact on the life cycle of an electrical asset, the optimization shall consider technical flexibility:

- Regarding PST taps, the optimization shall take into account a maximum frequency of tap changes in a given time interval define by each TSO or shall aim at minimizing the frequency of tap changes.
- Regarding topological RAs, the optimization shall take into account a maximum frequency of switching per element in a given time interval defined by each TSO or shall aim at minimizing the frequency of switching.
- Maximum number of curative RAs after contingency: Because there is a maximum time to activate curative remedial actions after the occurrence of a contingency, the optimization shall consider a maximum number of curative RAs per outage. Each TSO shall specify this number according to their own risk assessment.
- Curative RA associated to specific contingency: To activate a Curative RA, the contingency causing the constraint has to be in the observability area of the RA Connecting TSO. The occurrence of the contingency is then the trigger to activate the curative RA.
- Regarding PSTs, the active power flows through PSTs may be controlled in different modes, with the goal of optimising the network capacity and ensuring security in a determined region. This is valid for PSTs owned by TSOs but also for PSTs owned by third parties, which are not controlled directly by the TSOs. The operation modes can consist of tap or active power flow target and flow range. The operation mode influences the optimisation. In case of tap target mode, the optimisation shall consider as input tap range and shall provide as output tap setpoint. In case of active power flow target mode, the optimisation shall consider as input active power range and shall provide as output active power setpoint.

Cancellation or modification of the duration of a planned outage is, for the time being, considered non-costly RA. The TSOs shall provide its availability on a voluntary basis. If TSOs provide its availability, RAs shall be accordingly taken into account during the optimization.

In accordance with article 14(2) of CSAM, a remedial action can be designed as a combination of actions. In that sense, the optimization should also take this kind of remedial actions into account. The

remaining RAs related to Article 22 of SO guideline might be considered by each TSO when performing its local assessment regarding violation of voltage, short-circuit and stability operational limits. These actions are:

- control voltage and manage reactive power by means of:
    - tap changes of the power transformers;
    - switching of the capacitors and reactors;
    - switching of the power-electronics-based devices used for voltage and reactive power management;
    - instructing transmission-connected DSOs and significant grid users to block automatic voltage and reactive power control of transformers or to activate on their facilities the remedial actions set out in points (i) to (iii) if voltage deterioration jeopardises operational security or threatens to lead to a voltage collapse in a transmission system;
    - requesting the change of reactive power output or voltage set point of the transmission-connected synchronous power generating modules;
    - requesting the change of reactive power output of the converters of transmission-connected non-synchronous power generating modules;
- The following RAs listed in article 22 of SO Guideline will not be considered in the optimization, because they are not relevant to identify the most effective and economically efficient RAs for congestion management:
    - Inclusion of the normal or alert state manually controlled load-shedding;
    - Activation of frequency deviation management procedures;
    - Curtailment, pursuant to Article 16(2) of Regulation (EC) No 714/2009, the already allocated cross-zonal capacity in an emergency situation where using that capacity endangers operational security, all TSOs at a given interconnector agree to such adjustment, and re-dispatching or countertrading is not possible;
    - Re-calculation of day-ahead and intraday cross-zonal capacities in accordance with CACM guideline.

4.2.4. Time coupled optimisation

Taking into account that:

- Certain remedial actions, like generation units, have a minimum up-time/runtime or down-time taking more than 1 hour;
- Electrical equipment has limitation on number of switching actions per day,
- Operators can only manage a maximum number of topological changes between hours

Only the time-coupled optimisation can lead to a practical and least costly solution jointly considering all remaining hours of a day, and therefore is required.

For time-coupling optimisation, it is crucial to make use of constant identifiers for all relevant grid elements (as described in CGMM).

Depending on the timeframe the time-coupled optimisation taking into account technical, organisational and legal constraints should be performed for the 24h in day-ahead timeframe and for the remaining hours until the end of the day in the intraday timeframes. In accordance with Article 21 of the CE ROSC Methodology, the optimisation shall consider all constraints on XRAs, including intertemporal

constraints, when identifying the most effective and economically efficient XRAs for all timestamps that are being optimised.

In order to avoid dramatic changes and mitigate too high influence of the first hour(s), the optimiser should consider the result of the previous hours (e.g. from the previous day). In addition, in accordance with Article 21(4) of the CE ROSC Methodology, any constraints resulting from ordered XRAs in previous timestamps shall be taken into account in the optimisation.

4.2.5. Relieving operational security limit violations with balanced RAs

The optimisation shall identify XRAs to avoid overloads on XNES in base and contingency cases. A curative XRA may be used to avoid the overload in contingency case on an XNE as long as the temporary admissible transmission loading
(TATL) of the element is not exceeded. The overall optimization result after application of preventive and curative XRAs shall respect the permanent limits (PATL) of the XNEs.

In accordance with Article 22 of the CE ROSC Methodology, for addressing violations of other operational security limits, such as voltage violations, violations of short-circuit current limits or violations of stability limits, each TSO should perform local assessment and long-term operational security analysis. These violations may also be addressed during the coordination of XRAs. They may additionally be represented through system constraints.

In order to reassess the need of the Agreed but Not Ordered XRAs (ANORAs), ANORAs are removed from the CGM for the next CROSA. It allows to adjust the volume of costly measures and avoids unnecessary costs. The removed ANORAs are added to the list of available XRAs before the new optimisation is performed unless those removed ANORAs are no longer available for technical reasons.

Due to the possibility of re-dispatching of generation units, the cumulated fed-in active power into the electrical grid could change. To avoid this kind of behaviour and guarantee a balance between active power generation before and after optimisation the redispatch needs to be activated in a balanced way.

In case a removed ANORA has an influence on the balance of the grid, the subsequent optimisation needs to take this into account by reasonable means and ensure that the new proposed RAs are balanced in accordance with Article 25 of the CE ROSC Methodology.

4.2.6. Avoid additional violations of operational security limits on XNEs and scanned elements

The optimisation shall guarantee that no new operational security limits violations regarding current are created on XNEs and scanned elements nor existing ones are worsen. In case of scanned elements, the optimisation will take the threshold which is described in article 6 of Core ROSC into consideration.

To avoid unnecessarily constraining the optimisation, Central Europe TSOs may introduce an Admissible Further Loading Threshold (AFLT) applicable to scanned elements. The AFLT allows the recommended XRAs to increase the initial loading of a scanned element, as calculated prior to the optimisation, within the limits defined in accordance with Article 23 of the CE ROSC Methodology. The AFLT shall be applied in complement to the Virtual Positive Load Margin (VPLM) and the Permanent

Admissible Transmissible Loading (PATL) defined for the scanned element, according to Art. 23 (2) (a)..

In case a scanned element significantly constrains the optimisation process, the concerned Central Europe TSO may reassess the corresponding VPLM in order to reduce its constraining effect on the optimisation.

4.2.7. Minimise incurred costs

In accordance with the optimisation objective hierarchy defined in Article 24, the minimisation of incurred costs of RAs represents the second optimisation objective, applied after ensuring that operational security violations are relieved. The objective is to determine, among technically feasible solutions that ensure operational security, the set of RAs resulting in the lowest total incurred costs.

The total incurred costs consist of estimated costs incurred by costly RAs (e.g. Redispatching and countertrading) for congestion management, i.e. the estimation of incurred costs invoiced or credited by the providers of ordered costly RAs as defined in CE ROSC Methodology. It may include ramping costs, costs/revenues for balancing, and where applicable start-up costs and shut-down costs where CE TSOs agree to start or stop a generating asset to solve congestions.

The application of the economic efficiency principle, including the interaction between cost minimisation and the technical effectiveness of RAs, will be further assessed during the implementation phase, experimental operation, and actual operational use of the optimisation process. The predefined objective hierarchy will be monitored based on operational experience in order to identify whether any practical limitations or unintended effects occur. If such issues are identified, TSOs may develop and propose appropriate improvements to the optimisation approach.

4.2.8. RA effectivity

The objective of the CE RAO is to identify the most effective set of RAs to resolve operational security violations. The CE RAO shall take into account the impact of RAs on overloaded grid elements. This sensitivity factor shall be expressed in percentage of the maximum current of the concerned optimized grid elements. The optimisation resolves operational security violations while minimising the total cost of costly remedial actions. Therefore, the selection of RAs balances their effectiveness (sensitivity) and their associated costs, avoiding an excessive reliance on less effective actions solely to reduce costs.

During CROSA it will be indicated if a bidding zone/TSO is affected by a RA. This is required to determine the affected TSOs and required when a RA gets rejected.

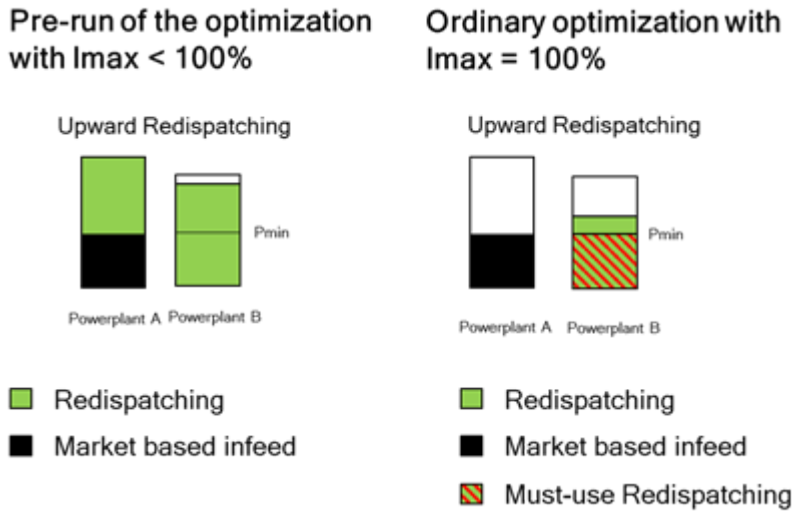
4.2.9. Robustness

In circumstances where the initial loading of XNEs is above its current limits, the result of the regional operational security coordination will lead to loadings on one or several XNEs very close to its current limits. Any variation for example of forecasts in consumption, RES production, market activities or unforeseen outages could lead again to overloads of the XNEs. In these situations, the CE TSOs must still have access to short-term potential of Remedial Actions to react on these overloads. Therefore, the solution of the regional operational security coordination shall not recommend additional RAs for these circumstances but shall, whenever possible, free them up in case they are needed. As example,

Redispatching in a short-term period could not be possible due to the fact, that the respective Power plant is offline and requires a too long lead time before it can be used for the demanded Redispatching. A robust solution could take this into account and finds results, where instead of one Power plant is fully used for Redispatching, two Power plants are used in each case with minimum power infeed.

A technical possibility to achieve a robust solution regarding Redispatching may be to perform a pre-run of the optimization, where the current limits of XNEs are reduced to a value smaller than 100%. Power plants which are started up for Redispatching and which cannot be re-evaluated in the next CROSA are “Must-use” Redispatching for the consecutive ordinary optimization at least with its minimum power. The consecutive ordinary optimization will use current limits without reliability margin in accordance with the applicable provisions of the CE ROSC Methodology and CSAM.

Example:



Other possibilities exist to reach this goal as among others:

1. considering additional margin respecting uncertainties to monitor and solve congestions,
2. ensuring that non-used RAs provide sufficient margin on highly loaded elements,
3. limiting the number of used actions in function of the time horizon of computation,
4. others…

During the implementation of the ROSC methodology, RCCs and TSOs will further assess and experiments the possibilities and amend the methodologies with the most appropriate solution

4.2.10 Coordination of XRAs

CE TSOs are allowed to reject recommended XRAs proposed by CE RCCs, in accordance to Article 27 of the CE ROSC Methodology. The following list includes some examples for a required rejection of a recommended XRA:

- power plants are currently not available;
- provided input data is not correct;
- a network element trips;
- violations of voltage or stability limits identified in local assessments;
- violations of operational limits in voltage levels below 220 kV identified in local assessments.

Normally, only the XRA connecting TSOs and XRA affected TSOs will have the right to reject the CROSA solution proposed by RCC. The rejection of a XRA by a TSO must not mean that the whole solution is rejected but only particular RAs. Such rejection may not imply new calculation. In case of rejection of XRAs connecting and/or affected TSOs with the support of CE RCCs shall identify and plan alternative XRAs taking into account cost and efficiency to relieve the operational security limits violations. CE RCC(s) may also recommend alternative XRAs.

If a CE TSO rejects a recommended XRA proposed by CE RCCs, the reasons shall be justified, documented by the relevant CE TSO(s) and provided to CE RCCs. A recommended XRA may be rejected when its implementation would result in operational security violations or when the XRA is no longer available.

In accordance with Article 27 of the CE ROSC Methodology, Central Europe RCC(s) in coordination with the respective Central Europe TSO may perform an ex-post assessment of rejected recommended XRAs in order to assess the additional costs and impact resulting from the rejection.

Output of coordination: As outcome of a CROSA, the list of Agreed XRAs is defined. This list identified the best estimation of the XRAs that will need to be used to relieve operational security violations on XNEs. When the foreseen time of a congestion and technical or other constraints allow so, TSOs might reassess the need to apply already Agreed XRAs during ID CROSAs. Based on updated CGM (including better load and generation forecast, unplanned outages etc.), RAO process may result in a need to increase or decrease the volume of certain XRAs (such as RD, CT or PST tap change) or not using the XRA at all and therefore find a more efficient and effective way to handle identified congestions. To be able to distinguish between Agreed XRAs which might yet be reassessed in next ID CROSA(s) and those which cannot be reassessed, CE TSOs have developed two terms to divide between Agreed XRAs which can or cannot be reassessed in next ID CROSAs:

- ANORA (Agreed but Not Ordered XRA) – their activation time allows reassessment in next ID CROSA and therefore steps leading towards their activation do not have to be made. ANORA is only the best estimate of a final solution that will be activated.
- Ordered XRA – cannot be reassessed later either due to its activation time or due to necessity to relieve a congestion forecasted to happen before next ID CROSA. Therefore steps leading to ORAs activation should be made. Only Fast activation process can lead to a change in Ordered RA.

4.2.11. Inter-CCR coordination

Article 46 of CSAM states that no later than eighteen months after the adoption of the CSAM, all TSOs shall jointly issue a request for amendment of the CSAM with rules for the identification and definition of overlapping zones, overlapping XNEs, overlapping XRAs, impacting CCRs and competent RCC(s), as well as, rules for the sharing of costs of the activated overlapping XRAs, in accordance with Article 27(3). This amendment will be the basis for Inter-CCR coordination, will be ready before the end of the implementation of the target solution for the CE ROSC and will be agreed among all CCRs.

The CE ROSC Methodology defines Inter-CCR coordination principles in Article 28. Central Europe TSOs and Central Europe RCC(s) shall relieve operational security violations on overlapping XNEs and shall coordinate overlapping XRAs impacting these overlapping XNEs. Central Europe RCC(s) shall also perform coordinated cross-regional operational security assessments with relevant other RCC(s).

The non-development of additional principles will not delay the implementation of the CE ROSC Methodology and in the meantime CE TSOs and CE RCCs will apply the bilateral or multilateral agreements that already exist between CE TSOs and other CCR TSOs or between CE RCCs and other RCCs.

4.3 Validation

4.3.1. Outcome of validation

After the validation session, Ordered XRA and ANORAS are known and can be logged and implemented in the IGM in accordance with Article 32.

It may happen that there are some remaining violations at the end of the validation session for several reasons, e.g.:

- the optimization didn't find enough XRA to remove every violation
- during the coordination of XRAs according to article 27, some XRAs have been rejected for relevant reasons
- some XRAs are not available anymore because of a contingency

In those situations, depending on when the violation is forecasted to happen, TSOs can propose new XRAs in the set of available XRAs, can look for XRAs coming from others CCRs, or can launch a Fast Activation Process.

The procedure for the determination of cross-border relevant XRA is largely dependent on the process step. The DA- or ID-CROSA will typically be characterized by the need to remove multiple congestions at the same time. As a result, a mix of non-costly and costly RAs can be expected, which must be understood as an overall measure to address all congestions. A clear allocation of individual measures, especially with regard to redispatching & countertrading, does not make sense.

Central Europe RCC(s) shall archive all Ordered XRAs and ANORAs after the validation session and report any remaining operational security violations. Based on this input, Central Europe TSOs shall specify the next steps, which may include, but are not limited to, an intraday CROSA or Fast Activation Process.

4.4. Implementation of remedial actions

4.4.1. Ordering and Activation of remedial actions

Respecting the results of last CROSA process, TSOs shall activate Agreed Remedial actions as close to real time as possible respecting their technical, operational, procedural and other constraints.The ordering of redispatching RAs may be performed as a change in active power output (ΔP) rather than as a target setpoint. Once ordered, RAs shall remain available for activation in accordance with the conditions defined during the ordering process.

To prevent intraday market trading further worsening the congestion and mitigating the relieving effect of the RA, the available cross-border capacities shall be updated. TSOs should not reduce available cross-border capacities unless it is considered that the N-1 security of the system is endangered. If it is, then only available capacities in the direction that worsens the congestions would be reduced. As example, in case of Countertrading or Redispatching between 2 control area, CE TSOs might reduce available cross-border capacity on the borders between these 2 control areas to prevent intraday market trading further worsening the congestion and mitigating the relieving effect of the RA. The Available cross-border capacity in directions not impacting the RA negatively shall not be modified.

When timings allow, Agreed RAs shall be included as inputs for subsequent operational processes, including IDCC and the preparation of IGMs.

4.4.2. Consideration of remedial actions in next IGM

Both the EU regulations (SO Guideline, CACM) and Methodologies (CGMM, CSAM) require that Agreed RAs shall be included in the IGMs and also shall remain distinguishable from the base ("clean") model. To be able to fulfil this requirement, CE TSOs aim to log all Agreed RAs in a platform separate from IGMs.

CSAM article 28 requires RCCCs to monitor inclusion of Agreed RAs into IGMs. To be able to do so, RCCs might for instance compare each TSOs IGMs against logged RAs and inform TSOs about identified inconsistencies.

Unlike ORA, the status of which won't be modified in subsequent ID CROSAs, the logged information about ANORAs will be used to remove those ANORAs from CGM and hence get a "clean" CGM. In this way, CE TSOs and RCCs will be able to correctly identify operational security violations and, where necessary, possibly propose more economically efficient and effective set of RAs.

4.4.3. Fast activation process

Fast Activation Process is defined as a process to relieve operational security limits violation where detection of this violation occurs either between or after the standard CROSA processes. In such a situation, fast activation of a RA is required and cannot wait for the next ID CROSA. For example, in case a sudden operational security limits violation arises close to real-time or in real-time (due to incorrect forecast, unplanned outage, unavailability of a RA etc.), a TSO has the responsibility to relieve the congestion as soon as possible. In case the RA meant to relieve the violation is not considered as XRA (has no cross-border impact), no coordination with RCCCs or neighbouring TSOs is needed. However, in case it concerns a XRA (the RA has cross-border impact), the Fast Activation Process will be applied. When doing so, the activation of this XRA shall be coordinated with impacted TSOs (in Normal or Alert system state). In Emergency system state, when a violation occurs, coordination is recommended where time allows it, pursuant to the provisions in CSAm. If time does not allow coordination, then affected TSOs would by only be informed about the activation as soon as practicable.

It might also happen that due to e.g. improved forecast, activation of a previously identified RA is no longer necessary, or only to a reduced extent. In such cases, affected TSOs may reassess the need of the (full) activation via Fast activation process. For example, cancelling a non-costly RA, such as topology change or PST tap change, might be very simple and easily done. However, cancelling RD or

CT RA could be quite difficult when the generators have already started ramping etc. Therefore, to decide whether to cancel activation of the RA, Affected TSOs have to carefully consider technical and operational feasibility and economic efficiency of doing so. In case that during such a reassessment, no agreement on an updated or alternative RA is produced, for operational security purposes, the previously agreed XRA retains its status as agreed and ordered and is activated.

Depending on time restrictions, RCCs could be asked to participate in the Fast activation process and should be at least informed about its outcome once the constraint has been successfully relieved. Once RAs to relieve the violation has been identified, coordinated and agreed, the Fast activation process ends. Lastly, all RAs agreed as a result of Fast activation process shall be taken into account in following IGMs. New operational security violations resulting from these RAs should be avoided.

5. IMPLEMENTATION

5.1. Monitoring

There are currently numerous existing European and national reporting and monitoring obligations regarding the management of the operational security of the interconnected grids. Further regulations for monitoring and reporting, also based on the internal electricity market regulation, have been already discussed.

With this background, it was crucial to analyse which reporting and monitoring requirements already existed in Italy North and Core CCR and whether these were sufficient to fulfil the reporting and monitoring requirements for CCR CE. Based on this, the additional needs have been discussed, as well as a mutual understanding of the processes and of the availability of the data. The meaningfulness and feasibility of the requirements have been analysed and the respective expenditure involved has been clarified, creating a synthesis of the former Italy North and Core CCRs requirements.

5.2 Implementation

As described in the SO Regulation and CSAM, when developing solutions for the application of Coordinated Regional Security Analysis, TSOs and RCCCs will consider the global efficiency and effectiveness. In this spirit, some of the functionalities and tools necessary for the ROSC need to be developed at regional and even pan-European level, RCCs taking into account related developments in other CCRs and system operation regions. Moreover, the CGMES format developed in accordance with the CGMM will be the basis for the target solution. Furthermore, the CE TSOs and RCCs shall aim at automatizing the optimisation step. Considering the different principles and the size of the CE region, this automatization will represent a challenge that should not be underestimated. Overall, the challenges and uncertainties behind the new processes and functionalities and the dependencies on parties, which are not part of the CE governance, need to be considered within a realistic timeframe for the implementation of the target solution.

Central Europe TSOs, with the support of Central Europe RCC(s), shall regularly provide information to Central Europe regulatory authorities regarding the implementation roadmap, implementation progress, implementation risks, mitigation measures and responsibilities related to implementation delays.

The CE ROSC Methodology shall be implemented in a stepwise manner, whereby each implementation step covers a defined portion of the overall scope of the methodology and each subsequent step expands the scope of the preceding step. Where appropriate, individual steps may implement simplified or interim versions of this overall scope, which shall be progressively refined in later steps.

By no later than six months after the approval of the CE ROSC Methodology, Central Europe TSOs and RCC(s) shall jointly develop an implementation framework describing this stepwise implementation approach and shall update it regularly.

The first implementation step(s) shall focus on the implementation of the Common CSA process for the day-ahead and intraday timeframes. The CSA implementation track shall provide for implementation in at least two steps:

1. a first implementation step covering DA coordination and the implementation of the ID CSA process, including hourly ID RSA and an initial implementation of ID coordination; and
2. subsequent implementation step(s) further extending and completing the implementation of ID coordination, taking into account the progress and experience gained from the first implementation step.

The purpose of these implementation steps is to establish and progressively extend a common regional process supporting the exchange and validation of operational data, the assessment of operational security, the coordinated management of remedial actions and the implementation of agreed actions.

The common CSA process consists of the following high-level activities:

Day Ahead:

1. Input data preparation and validation
    - TSOs provide the operational data required for the execution of the CSA process.
    - The provided data is subject to consistency and quality checks prior to its use in the coordination process.
    - Common Operational security analysis Operational security assessments are performed by RCCs using the latest available network models and operational data.
    - The objective is to identify actual or forecast operational security violations requiring coordinated action.
2. Common Remedial action proposal and coordination of all CE TSOs
    - Available remedial actions are manually assessed and coordinated among the concerned TSOs.
    - The coordination process aims at identifying an agreed set of remedial actions capable of addressing the identified operational security violations.
3. Common Validation of results by all TSOs
    - The results of the coordination process are validated by the participating TSOs and RCC(s).
    - Agreed remedial actions and any remaining operational security violations are recorded and communicated.

Intraday:

1. Common hourly Regional Security Analysis

- Input data preparation and validation
  Operational security analysis are performed by RCCs, using the latest available network models and operational data to identify changes in actual or forecast operational security violations

2. Intraday reassessment
   - Coordinated reassessment in intraday following the ICS FAP principles is carried out.
   - During the intraday timeframe, previously agreed actions may be reassessed using updated operational information.
   - This allows the coordination process to reflect changing system conditions and to maintain operational efficiency.

Implementation of agreed remedial actions:

- Agreed remedial actions are implemented in accordance with their operational characteristics and activation requirements.
- The resulting network state is reflected in subsequent network models and coordination processes.

The detailed implementation scope, sequence and timing of these activities shall be in the implementation framework. For the CSA implementation track, the framework shall identify the relevant tasks, milestones and deliverables, including those for which each Central Europe TSO and RCC is individually responsible and those for which Central Europe TSOs and RCC(s) are jointly responsible.

The implementation framework shall also describe subsequent optimisation activities concerning RAO and CS, including, where available, their envisaged sequencing, indicative outputs and indicative timelines. This information shall be indicative and subject to the assumptions, dependencies and outcomes of the activities identified in the implementation framework and shall not constitute a commitment to specific implementation dates, milestones or go-live dates.

The implementation framework shall identify the main assumptions and dependencies underlying the implementation timelines, including dependencies related to procurement and the outcome of the relevant tender process. Where these assumptions or dependencies materially change, the corresponding target dates and implementation planning shall be reassessed and, where appropriate, reflected in an update of the implementation framework.

Central Europe TSOs and RCCs shall also regularly share information on the development of their tools, systems and processes with TSOs and RCC(s) of the South East Europe CCR in order to facilitate the future implementation of similar solutions in that CCR. The sharing of such information is conditioned on unanimous agreement of the CE TSOs.

After adoption of this ROSC Methodology and during its implementation, Central Europe TSOs and Central Europe RCC(s) shall endeavour to continue to improve the existing Central Europe CSA and the existing day-ahead and ID RSA processes.

6. ALLOCATION OF TASKS BY RCCS

The elements that need to be described under the organisation of regional operational security coordination are further defined in article 77(1) of SO Regulation.

It should also be considered that on 4th July 2019 Electricity Market Regulation (EMR) entered into force that also contains in Art. 37 EMR tasks that shall be performed by regional coordination centres and references to SO Regulation. As a consequence, SO Regulation needs to be interpreted in the light of EMR and should not be considered as a stand-alone regulation.

6.1 Appointment of RCCs and delegation of tasks to RCCs

The Article 38 covers the formal appointment, by CE TSOs, of all RCCs that will perform the tasks listed in the article 77(3) of the SO Regulation, allocated by the model that shall be defined before formal approval of CE ROSC Methodology.

TSOs of CE CCR are shareholders of two separate RCCs, which are CORESO and TSCNET. Consequently, CORESO and TSCNET have been appointed as CE RCCs to perform the tasks listed in the article 77(3) of SO Regulation and listed in Article 38.

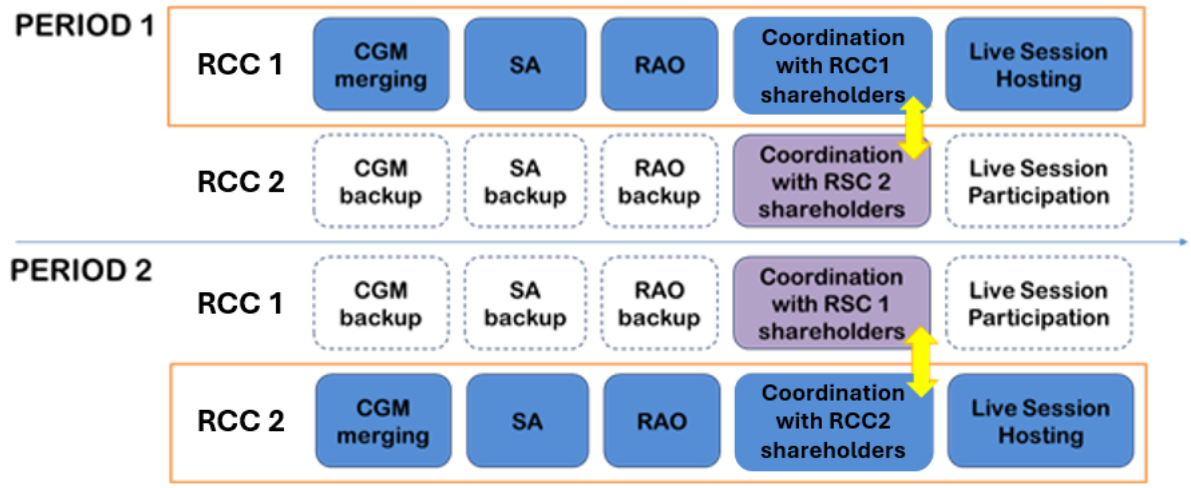
6.2 Allocation of tasks between RCCs

Article 39 is describing how the tasks listed in article 38 are allocated between Coreso and TSCnet.

Regional operational security coordination

Regional operational security coordination will be carried out based on a Rotational Operating Model. In case of the **Rotational Operating Model**, two (or more) RCCs carry out a task on a rotational/alternating basis, while both (all) RCCs have a role in the process at each rotation period. The Leading RCC of a specific rotation period has the overall responsibility for the whole process, carries out the process and shares the output with the other RCC(s). For the parts of the process that require specific expertise on each TSO's grid and/or coordination/communication with the TSOs, the Backup RCC contributes with its expertise to support the Leading RCC, whenever needed. The Backup RCC has the overall responsibility to act as a redundant RCC for the Leading RCC whenever needed.

Example of the Rotational Model applied on CSA process:



The roles and the responsibilities of the Leading and Backup RCC are the following:

- Leading RCC:
  - is legally and operationally responsible and accountable for the successful start, execution and conclusion of the process (both in Day Ahead and Intraday timeframe);
  - ensures that all the steps of the process are fulfilled: delivery of data sets by TSOs, start and finish of each process step, reporting and communication of process results.
- Backup RCC:
  - facilitates coordination with the TSOs that are non-shareholders of the Leading RCC; each TSO maintains their contact with their RCC;
  - supports the Leading RCC in the design and proposal of sets of RA;
  - acts as redundancy to the Leading RCC in case of stressed situations on the network and inability of the Leading RCC in executing the process.

For the Rotational Model, Coreso and TSCNET will define the pre-defined period when establishing the high-level business solution referred to in article 40(4)(a) (for example weekly rotation). This predefined period can be modified by RCCs and TSOs if it is deemed more efficient.

Common grid model building

Within ENTSO-E, TSOs will set-up a consistent and harmonized approach at pan-European level to ensure that the solutions implemented to build Common Grid Models and operated by RCCs will be compliant with the respective requirements set up in the relevant legislation in force, including SOGL Regulation (notably Article 79(5)), the CGM methodology and the CSA methodology, while ensuring reliability of the CGM delivery process and the aligned use of the resulting unique CGM.

According to SOC decision (04/12/2019) RCCs shall participate in the CGM building process on a rotational principle, with regular building and provision of a CGM by one main RCC and one backup RCC at all times. In addition, each RCC shall check the quality of the IGMs, according to Article 79(1) of the SO Regulation.

Regional outage coordination and regional adequacy assessment

OPC and STA tasks are already provided by CE RCCs in accordance with methodologies developed in ENTSO-E for implementation of articles 80 and 81 of SO Regulation.

6.3 Assessment of the effectiveness and efficiency

The initial assessment of the effectiveness and efficiency of the proposed setup with the rotational model is included in Appendix 1 of the present Explanatory Note.

Article 40 defines the requirements how the effectiveness and efficiency will be monitored. ENTSO-E has to prepare each year by 30 September an annual report on regional coordination assessment based on the annual reports on regional coordination assessment provided by the regional security coordinators. The report has to assess any interoperability issues and propose changes aiming at improving effectiveness and efficiency in the system operation coordination according to SO Regulation Article 17, based on the reports prepared by RCCs.

CE TSOs in coordination with CORESO and TSCNET shall monitor the effectiveness and efficiency of the allocation of the tasks for which they are responsible and, where applicable, the rotation of those tasks and their operational performance.

CE TSOs in coordination with CORESO and TSCNET shall agree on clear and specific performance indicators for the tasks referred to in Articles 38 and 39.

RCCs will be faced with increased reporting obligations based on Art. 46 EMR. RCCs shall establish a process for the continuous monitoring of at least: (a) their operational performance; (b) the coordinated actions and recommendations issued, the extent to which the coordinated actions and recommendations have been implemented by the transmission system operators and the outcome achieved; (c) the effectiveness and efficiency of each of the tasks for which they are responsible and, where applicable, the rotation of those tasks. Furthermore, RCCs shall submit an annual report on the outcome of the monitoring about this information on their performance to the ENTSO-E, ACER, the regulatory authorities in the system operation region and the Electricity Coordination Group. RCCs shall report any shortcomings that they identify in the monitoring process to the ENTSO-E, the regulatory authorities in the system operation region, ACER and the other competent authorities of Member States responsible for the prevention and management of crisis situations.

When preparing the reports, RCCs will have to detect the issues reducing the effectiveness and efficiency of the processes, allowing to suggest improvements in processes and allocation of tasks between the RCCs, covering also the requirements of Article 77.

CORESO and TSCNET shall ensure, in consultation with the Central Europe TSOs, transparency and interoperability of all processes and the associated data within the operational tasks. CORESO and TSCNET shall assess interoperability issues and propose changes aiming at improving effectiveness and efficiency in the coordination of system operation.

6.4 Decision-making process and governance

Coordination decision-making processes and governance will be further defined in the High-level business solution defined during the implementation of the CE ROSC Methodology, which details the cooperation between RCCs and the contractual framework between CE RCCs and TSOs.

All Central Europe TSOs shall cooperate for the implementation and operation of the CE ROSC Methodology through common bodies where each TSO shall have at least one representative. The members of these common bodies shall aim to make unanimous decisions.
A steering committee consisting of one representative from each Central Europe TSO shall make binding decisions on matters related to the implementation and operation of the CE ROSC Methodology. The steering committee shall also act as a body for settlement of disputes among Central Europe TSOs regarding the implementation and operation of the methodology.

The steering committee shall resolve disputes related to the interpretation, design, implementation and operation of the methodology where such matters are not otherwise defined in the methodology itself.

RCCs shall cooperate in good faith and shall seek to adopt a fair and loyal treatment of the other parties concerned. RCCs shall implement the provision of the tasks in close consultation and cooperation with the Central Europe TSOs. RCCs and Central Europe TSOs shall establish a contractual framework for the implementation of the methodology.

The responsibility for secure system operation and for any decision taken based on tasks performed by CORESO and TSCNET shall remain with the Central Europe TSOs according to applicable laws and regulations.