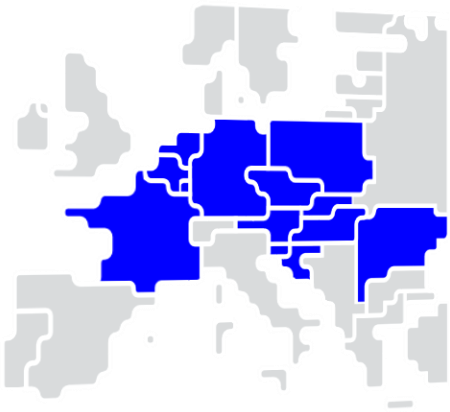
CCR Core TSOs' Cooperation

Explanatory document to the Core 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"

19 December 2019



Disclaimer:
This document is released on behalf of the transmission system operators ("TSOs") of the Capacity Calculation Region Core 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

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 Core Transmission System Operators (hereafter referred to as “Core TSOs”) submitted the Common Methodology for Regional Operational Security Coordination for the Core Capacity Calculation Region (hereafter referred to as “Core CCR”) to Core NRAs. This methodology aims at the day-ahead and intraday regional operational security coordination within the Core CCR.

The aim of this explanatory note is to provide additional information with regard to the Methodology for Regional Operational Security Coordination for the Core CCR (hereafter referred to as “Core ROSC Methodology”). In particular, it provides insight on the whole process chain defined in Core ROSC Methodology, from the preparation of input data to the optimisation and implementation of Remedial Actions. 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 Core ROSC Methodology.

- Operational security constraints are most commonly current, short-circuit, voltage or stability constraints.
  The Core ROSC Methodology 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. For the detection of other constraints, such as voltage violations, violations of short-circuit current limits or violations of stability limits, each Core 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.

- 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 too 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
  - 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-Core TSO, etc.
  - Legal constraints mean the legal requirements stated in national laws regarding 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.

- 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 system constraints shall share transparently with Core RSCs and TSOs the information justifying their application.

2. REGIONAL OPERATIONAL SECURITY COORDINATION

As illustrated in figure 1, the Core 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 and several intraday Coordinated Regional Operational Security Assessment (hereafter referred to as 'CROSA').
- Intraday CROSAs shall be performed at least three times in intraday timeframe in accordance with article 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 RSCs and TSOs.

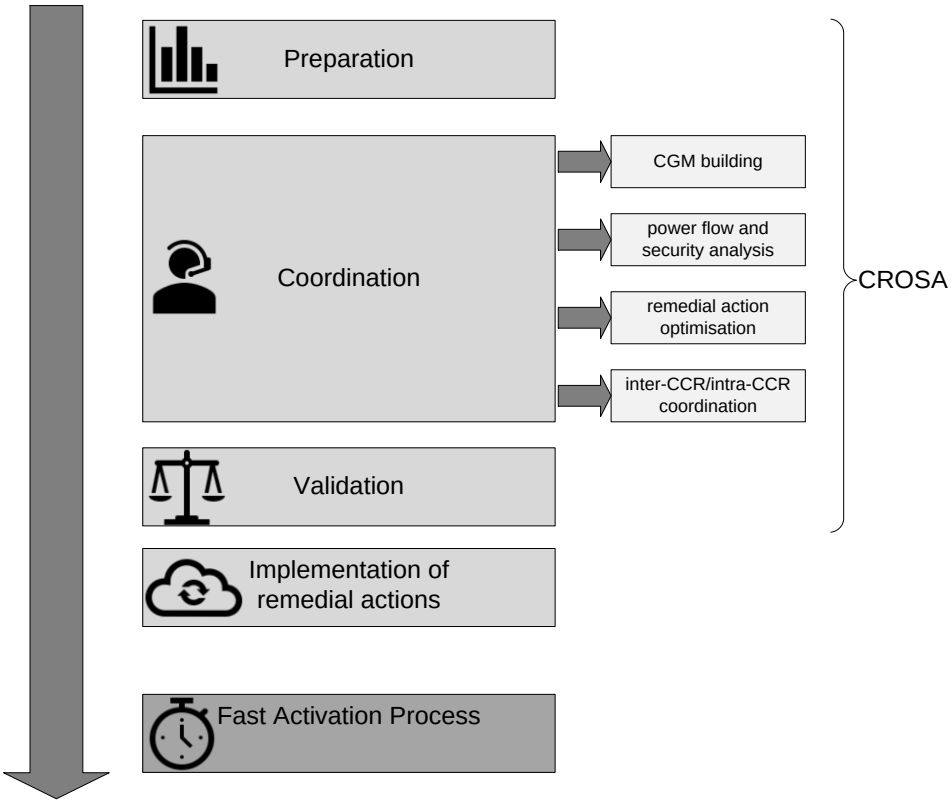


Figure 1: Overview Coordinated Regional Operational Security Assessment (CROSA) process

On top of the ROSC process, Core TSOs with Core RSCs shall perform intraday regional security analysis ('ID RSA'). The goal of the ID RSA is to provide Core 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 CORE 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 Secured 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 **Secured element** 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.

Having this in mind, Core TSOs decided that **secured elements are the elements identified as cross-border relevant network elements** (XNEs) in accordance with CSAM within the Core CCR.

Core 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 Secured elements 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, Core TSOs decided to consider all elements with voltage level equal or higher than 220kV as XNEs (Core XNEs) and decided to define criteria for which certain elements can be discarded as XNE.

If one of the following criteria is fulfilled, Core TSOs shall have the right to exclude elements from the set of secured elements:

- 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 set of secured elements in accordance with the provisions explained above.

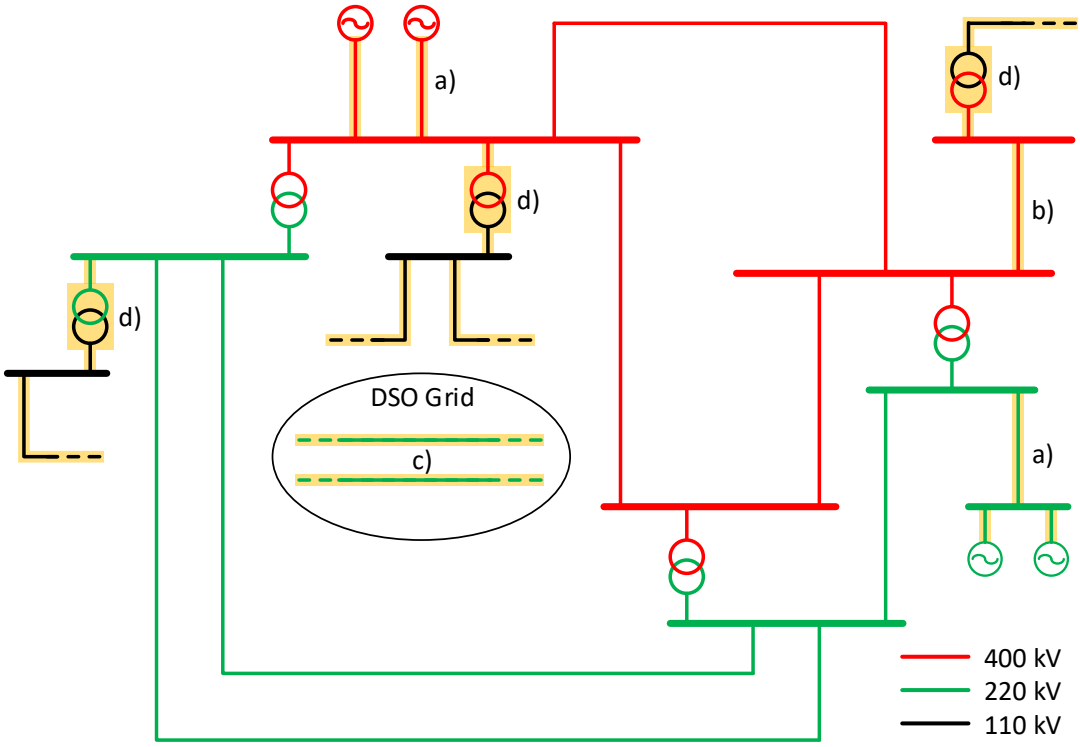


Figure 2: Elements (highlighted in yellow) which can be discarded from the set of Core XNEs

- In addition to these criteria, any element can be discarded from the set of secured elements, when a common agreement among Core 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 Core CCR and XBRNEs in accordance with the Core RD and CT methodology.

TSOs which are part of more than one CCR shall have the right to discard any of their elements from the set of secured elements which are regarded as XNE in another CCR.

As suggested by ENTSO-E, Core TSOs define scanned elements as set of elements on which the CROSA shall not create new operational security limits violations or worsen any existing violation. Such elements can be elements which are discarded from the set of secured elements 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 secured elements). Such an inclusion must be compliant with the CGMM.

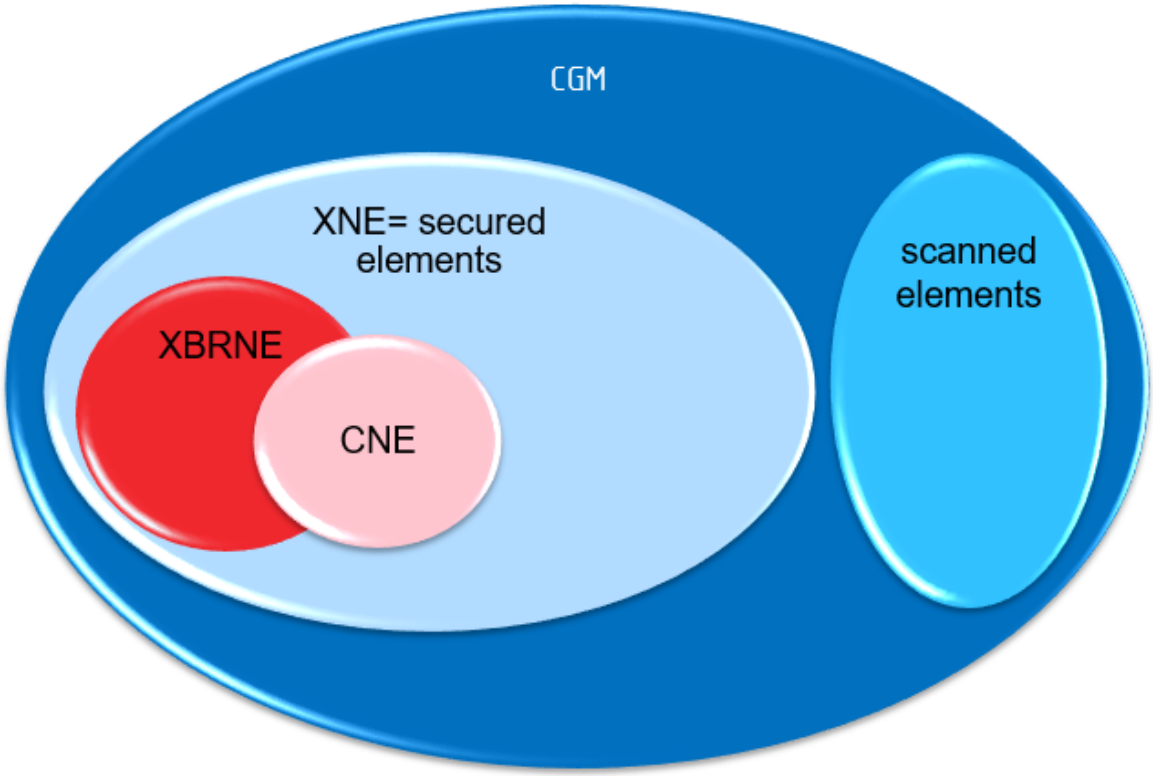


Figure 3: secured and scanned elements

Core TSOs shall have the right to update the lists of secured 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 secured element by default and therefore any new element at such a voltage level can be included in this list of secured elements.
- Discarding an element from the list of secured elements is subject to common agreement by Core TSOs, except for those elements, that fulfil one of the criteria defined in this chapter.
- Any discarded element from the list of secured elements can be included in the list of scanned elements, but it is not mandatory.
- Each Core 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 secured elements.
- Each TSO shall have the right to include any new element with a voltage level lower than 220kV in the list of scanned elements providing justification for its inclusion. Such elements have to be modelled in IGM.

Core TSOs shall have the right at any time to exclude any element from the set of scanned elements. Core TSOs shall update the secured elements list and scanned elements list when necessary and inform the RSC about the change. Both lists shall be reassessed by each Core TSO at least once a year.

Lists of secured and scanned elements will be made available before each CROSA process.
Each Core 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 Core TSO has to prepare a list of remedial actions which can be used to relieve at least violation of the Core TSO's current limits. Core 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, Core TSOs shall share with Core RSCs 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, Core 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.

3.3 Cross-border relevance of remedial actions

The CSA methodology defines a cross-border remedial action (XRA) as a RA identified as cross-border relevant and which needs to be applied in a coordinated way. The cross-border relevance of a RA shall be evaluated qualitatively or quantitatively for at least each cross-border relevant network element and each contingency.

Considering the definition of Core XNEs, it is obvious that some RAs will only have a relevant impact on XNEs located in the same control area and will de facto only affect its connecting TSO. Nevertheless, these remedial actions will still be named “cross-border relevant” and flagged as XRAs. However, during the fast activation process, the activation of such XRA by the connecting TSO will not be subject to further coordination.

3.3.1 Qualitative assessment of XRAs

Core 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. This process consists of the following steps:

- In order to assess if a RA is cross-border relevant, each Core TSO shall assess the impact of the RA on its control area.
    - This assessment can be based on operational experience, but it is not limited to it;
- In order to assess the cross-border relevance of the RA, the RA Connecting TSO shall assess the impact on the control area of other TSOs;

  - It is needed to assess relevance of the RA on the grid of other TSOs and on its own grid in order to compare the results among TSOs, as TSOs might have different views on certain RAs. This can be expected when quantities for redispatch or tap positions of PSTs will be assessed.
- If the RAs are quantifiable such as redispatching, countertrading, change of set point on HVDC systems or change of taps on phase-shifting transformers, the quantity above which this RA is deemed cross-border relevant on the grid of other TSOs and its own grid has to be specified.
  - In case of PST number of TAPs or change in the flow can be specified
  - In case of redispatching, the amount for internal redispatching and the amount per TSO/TSO border shall be specified.
  - In case of HVDC change from set point shall be specified.
- Core TSOs will share the results of the assessment and provide justifications to connecting TSOs why RAs have been selected as relevant.
- If common agreement is reached among Core TSOs, then RA is defined as cross-border relevant and affected TSOs will be identified.
- If a RA is not proposed as cross-border relevant by any Core TSO, it is considered as non-cross-border relevant.
- If a RA is identified as cross-border relevant only for the RA Connecting TSO, this TSO shall be considered as the only XRA affected TSO.

3.3.2 Quantitative assessment of XRAs

In case that Core 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

Core TSOs shall use the common grid models established in accordance with article 67 of the SO Regulation when computing remedial action influence factor.

If a RA consists of a combination of actions, its cross-border relevance shall be assessed for the effect of the combination. All remedial actions which have influence facto greater than the threshold defined in article 15 (5)[1] of CSAM shall be considered as cross-border relevant, otherwise RAs shall be considered as non-cross-border relevant. All Core TSOs that have at least one affected XNEC for which the remedial action influence factor is greater than the threshold shall be considered as XRA affected TSOs,

TSOs shall delegate tasks described above to their respective Core RSCs.

- 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 CORE TSOs and will be provided to Core RSCs.
- Reassessment of the list of cross-border relevant RAs shall be done on a yearly basis. Nevertheless, each Core 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 Core RSCs.

[1] 5%

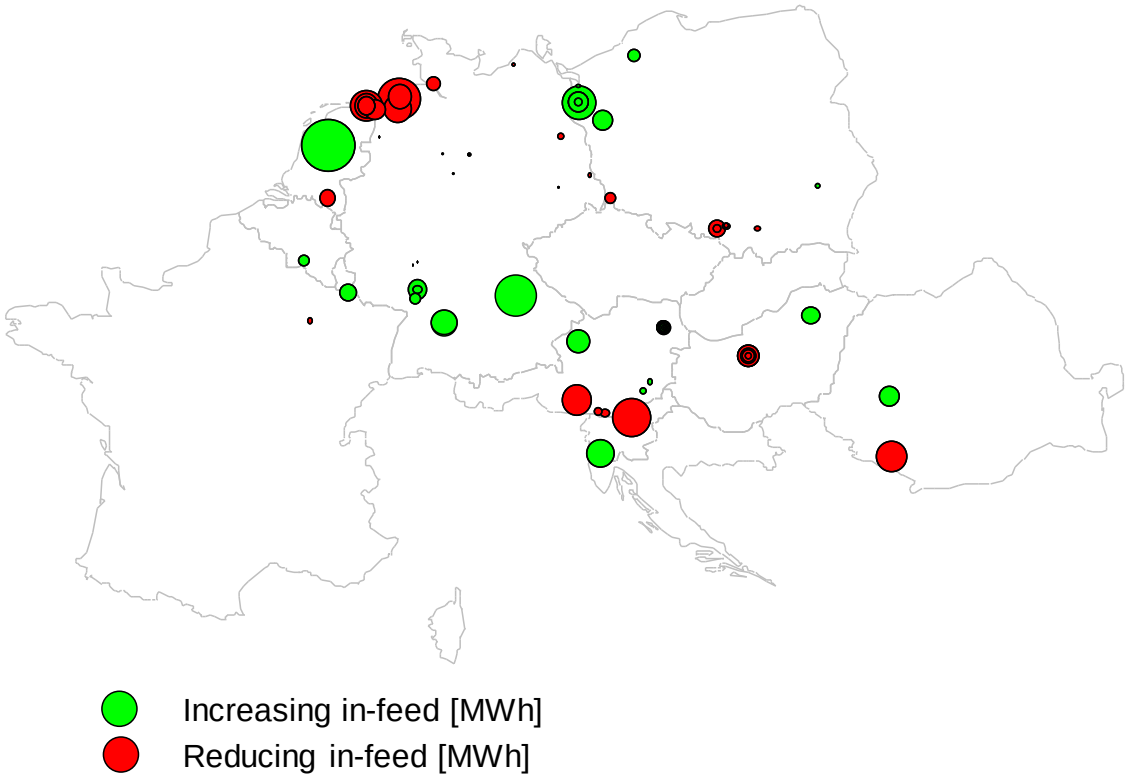


Figure 4: Exemplary result of a Core-wide Redispatching optimization

In the CROSA process step it can only be analysed which TSOs are affected by the application of the determined whole solution by determining the effect of the overall solution on the XNEC of each TSO. If the influence factor of the overall CROSA solution on given XNEC, calculated in the same way as for determination of XRAs, is greater than the threshold defined in article 15 (5) of CSAM, than the XNEC is considered affected. Core TSO which have at least one affected XNEC will be than considered as CROSA affected TSO. All CROSA affected TSOs and RAs 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 Core 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 Core ROSC. In the case of a lack of agreement, a quantitative determination as in Article 12 of Core 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 RSC.

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 Core TSO should prepare a contingency list only with elements relevant for Core CCR and used in Core 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 Core RSCs unless contingency on that element can endanger the operational security limits on the secured or scanned elements defined in Core CCR.

Such established contingency list should be made available to both Core RSCs and Core 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. RSCs 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.

4. COORDINATED REGIONAL OPERATIONAL SECURITY ANALYSIS PROCESS

4.1 Preparation

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

- IGMs in line with the CGM methodology, including the operational security limits for each secured or scanned element;
- Available remedial actions within his control area;
- When relevant, System Constraints;
- Secured and scanned elements;
- Contingency list

The input data shall cover all hours for a business day related to intraday and day-ahead CROSA means 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.

Core 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, Core TSOs shall re-assess their availability and consider the agreed outcome of previous optimisations in accordance with Article 16 of CORE ROSC Methodology.

When receiving any input data, the Core RSC shall perform a quality and consistency check aiming at identifying any format error or any inconsistency with the information contained in the IGMs. The Core RSC shall then report these errors to the Core 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 22 to 32 of the Core ROSC Methodology.

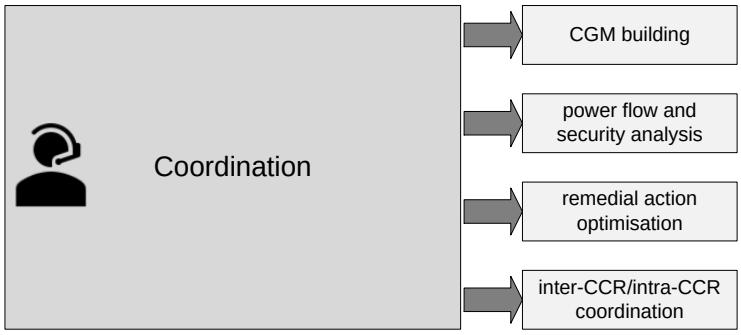


Figure 5: Overview coordination process

The day-ahead CROSA includes two of those coordination runs. There will be at least three ID CROSAs and each will include at least one coordination run. 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 Core TSOs but also by the other CCRs and non-Core TSOs.

Intra-CCR coordination describes the coordination between Core TSOs and Core RSCs, inter-CCR coordination means the coordination between Core TSOs and RSCs with the TSOs and RSCs of other CCRs.

4.2.2. Power flow and security analysis

The validation aims at identifying input mistakes which would make the outcomes of the operational security analysis non-realistic to give Core TSOs the opportunity to correct these errors. It doesn't mean that TSOs have to perform a power flow and security analysis on their own and then compare the results to validate them.

4.2.3. Optimisation of remedial actions

An optimization of RAs has to be done in order to identify in a coordinated way the most effective and economically efficient RAs. 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 25 (3) of Core 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 Core TSOs and Core RSCs.

Main goal of the optimisation process and part of the CROSA is that each TSO shall maintain current (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.

The optimization should be able to identify RAs 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 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 till the end of the day in the intraday timeframes. 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).

4.2.5. Relieving operational security limit violations with balanced RAs

The optimisation shall identify RAs to avoid overloads on secured elements in base and contingency cases. A curative RA may be used to avoid the overload in contingency case on a secured element as long as the temporarily limit (TATL) of the element is not exceeded. The overall optimization result after application of preventive and curative RAs shall respect the permanent limits (PATL) of the secured network elements.

In order to reassess the need of the Agreed but Not Ordered RAs (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 RAs 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 28.

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

The optimisation shall guarantee that no new operational security limits violations regarding current are created on secured 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 (1) of Core ROSC into consideration.

4.2.7. Minimise incurred costs

Because all incurred costs of applied costly RAs has to be incurred by TSOs, regardless of applied payment principle (i.e. requester pays or polluter pays), as it is also required by SO guideline that the CSA outcome has to be “most effective and economically efficient”, the minimisation of RAs incurred costs should be a principle of the optimisation. The most effective and efficient activation of RA is depending on the location of the overload, actual availability and location of RAs.

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 Core RD and CT Methodology. It may include ramping costs, costs/revenues for balancing, and where applicable start-up costs and shut-down costs where Core TSOs agree to start or stop a generating asset to solve congestions.

4.2.8. RA effectivity

With the objective to determine the most effective set of remedial actions, the Core RAO when considering the selection of an individual costly or non-costly remedial action, shall consider the sensitivity of these actions on each of the overloaded optimized grid elements. This sensitivity factor shall be expressed in percentage of the maximum current of the concerned optimized grid elements.

For costly RA, the sensitivity of any change of power on a generating unit shall require a definition of the compensation. This will be defined during the implementation.

The objective to minimize the total cost of costly remedial action will lead to the fact that, at identical sensitivity, a less costly RA shall always be preferred to one with higher costs. But using low effective RA to solve far away congestions might also have side effects in term of grid stress and reduction of available means close to their activation. The exact ratio between cost and sensitivity might have to be tuned in order to avoid over-used of far and less sensitive non-costly remedial action just to provide limited gain in the incurred costs.
The main driver of the optimisation, as part of the CROSA process, is the security of supply by finding the most optimal set of RAs taking into account their effectivity and efficiency.

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.

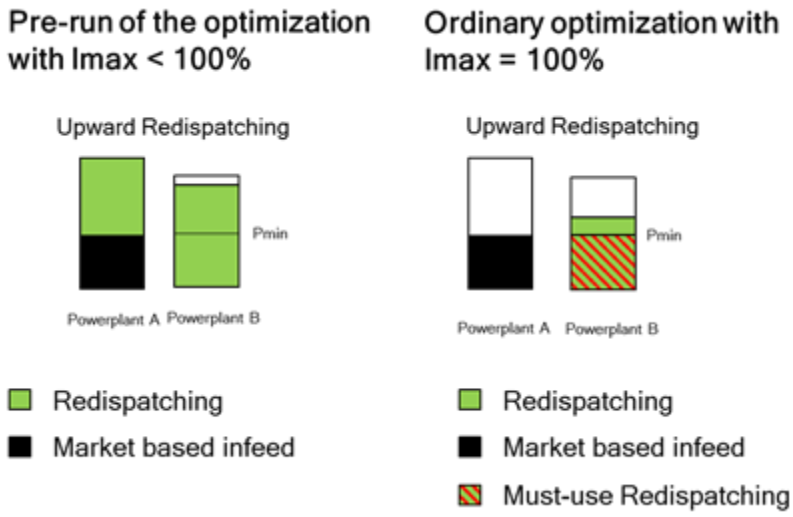
4.2.9. Robustness

In circumstances where the initial loading of secured elements is above its current limits, the result of the regional operational security coordination will lead to loadings on one or several secured elements 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 secured elements. In these situations, the Core 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 secured elements 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 to CSAM Article 23 (1)(a) and CSAM Article 24 (3)(a).

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, RSCs and TSOs will further assess and experiments the possibilities and amend the methodologies with the most appropriate solution

4.2.10 Coordination of RAs

Core TSOs are allowed to reject RAs proposed by Core RSCs. The following list includes some examples for a required rejection of a RA:

- 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 RA connecting TSOs and CROSA affected TSOs (as described in p. 3.3.2) will have right to reject the CROSA solution proposed by RSC. The rejection of a RA 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 RAs connecting and/or affected TSOs with the support of Core RSCs shall identify and plan alternative RAs taking into account cost and efficiency to relieve the operational security limits violations.

If a Core TSO rejects a RA proposed by Core RSCs, the reasons shall be justified, documented by the relevant Core TSO(s) and provided to Core RSCs.

Output of coordination: As outcome of a CROSA, the list of Agreed RAs is defined. This list identified the best estimation of the RAs that will need to be used to relieve violation of flow operational security limits on Secured elements. When the foreseen time of a congestion and technical or other constraints allow so, TSOs might reassess the need to apply already Agreed RAs 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 RAs (such as RD, CT or PST tap change) or not using the RA at all and therefore find a more efficient and effective way to handle identified congestions. To be able to distinguish between Agreed RAs which might yet be reassessed in next ID CROSA(s) and those which cannot be reassessed, Core TSOs have developed two terms to divide between Agreed RAs which can or cannot be reassessed in next ID CROSAs:

- ANORA (Agreed but Not Ordered Remedial Actions) – 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 Remedial Actions – 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 RSC(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 Core ROSC and will be agreed among all CCRs. Therefore, Core TSOs decides not to develop Inter-CCR coordination principles in the meantime because such principles will never be implemented before the CSAM amendments and Core TSOs cannot enforce such principles on other CCRs. The non-development of such principles will not delay the implementation of the Core ROSC Methodology and in the meantime Core TSOs and Core RSCs will apply the bilateral or multilateral agreements that already exist between Core TSOs and other CCR TSOs or between Core RSCs and other RSCs.

4.3 Validation

4.3.1. Outcome of validation

After the validation session, Ordered RA and ANORAS are known and can be logged and implemented in the IGM in accordance with article 36.

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 RA to remove every violation
- during the coordination of RAs according to article 31, some RAs have been rejected for relevant reasons
- some RAs are not available anymore because of a contingency

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

The procedure for the determination of cross-border relevant RA 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.

4.4. Implementation of remedial actions

4.4.1. 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.

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, Core 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 won't be modified. When timings allow, Agreed RAs will figure as inputs for the ID CC process (incl. 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 put into IGMs and also shall be distinguishable from the base ("clean") model. To

be able to fulfil this requirement, Core TSOs aim to log all Agreed RAs in a platform separate from IGMs. CSAM article 28 requires RSCs to monitor inclusion of Agreed RAs into IGMs. To be able to do so, RSCs 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 next 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, Core TSOs and RSCs will be able to correctly identify congestions and possibly propose more 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 RSCs 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 only if time allows it. If not, then affected TSOs would by only be informed about the activation.

It might also happen that due to e.g. improved forecast, activation of certain RA is no longer necessary. In such cases, affected TSOs may reassess the need of the 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.

Depending on time restrictions, RSCs 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 activated as a result of Fast activation process shall be taken into account in following IGMs. New congestions as a result of these RAs should be avoided.

5. IMPLEMENTATION

5.1. Monitoring

There are currently numerous existing European and national reporting and monitoring obligations regarding RD and CT. Further regulations for monitoring and reporting, also based on the internal electricity market regulation, are currently being discussed.

With this background, it is crucial to analyse which reporting and monitoring requirements already exist and whether these are sufficient to fulfil the reporting and monitoring requirements for CCR Core. Based on this, the additional needs have to discuss. This should be done in workshops in order to create mutual understanding of the processes as well as of the availability of the data, to discuss the meaningfulness and feasibility of the requirements and to clarify the respective expenditure involved. Thus, an efficient implementation of the necessary reporting and monitoring can take place.

5.2 Implementation

As described in the SO Regulation and CSAM, when developing solutions for the application of Coordinated Regional Security Analysis, TSOs and RSCs 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, by taking into account also initiatives from other regions for which at least Core RSCs will be responsible. Moreover, the CGMES format developed in accordance with the CGMM will be the basis for the target solution. Furthermore, the RSCs will aim at automatizing the optimisation step. Considering the different principles and the size of the Core 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 Core governance, need to be considered within a realistic timeframe for the implementation of the target solution.

In this respect, Core TSOs and Core RSCs have decided to describe in the Core ROSC Methodology the different steps that will be necessary for the definition, the development and the testing of the target including an estimation of the maximum time for each step.

As the maximum timing of some of the steps will also be highly dependent of the development phase and is fixed when the contracts with the vendors are signed, it is also proposed to review and amend these timing in the Methodology once the tendering process for the different tools and hardware is finished.

Nevertheless, considering the importance to improve the efficiency of the coordination at the regional level, Core TSOs and Core RSCs are aware and convinced that they cannot wait for the full implementation of the target solution. This is the reason why they also engage themselves to define and develop a stepwise approach considering interim solutions in a more ambitious but still realistic timing and to amend the Core ROSC Methodology before 1 year after its approval accordingly. This stepwise approach and related interim solution shall be based on the following principles:

1. Improve the current level of coordination on Core regional level, i.e. that the stepwise approach will respect the spirit and ambition of the provisions as defined in the Core ROSC Methodology regarding the determination and activation of Agreed remedial actions and not develop a sub-regional solution;
2. Shall consider existing processes and tools without delaying the implementation of more advanced regional or pan-European solutions or processes when necessary, i.e. the interim solution might use the existing UCTE format and move to the CGMEs format once this will be proven robust at pan-European level or might use a much simpler way to exchange and report data and results;
3. Shall be implemented faster and more ambitious, but within a realistic timing, i.e. Core TSOs and Core RSCs expect this interim solution implemented in less than 24 months and
4. Shall require reasonable implementation effort, i.e. the required time and costs for the development and implementation of an interim solution have to be taken into account.

The Core ROSC Methodology shall be implemented in a consistent manner with the Core RD and CT Methodology and Core Cost Sharing Methodology.

6. ALLOCATION OF TASKS BY RSCS

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 security coordinators (in the future 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 RSCs and delegation of tasks to RSCs

The Article 41 covers the formal appointment, by CORE TSOs, of all RSCs 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 Core ROSC Methodology.

TSOs of Core CCR are shareholders of two separate RSCs, which are CORESO and TSCNET. Consequently, CORESO and TSCNET have been appointed as Core RSCs to perform the tasks listed in the article 77(3) of SO Regulation and listed in Article 41.

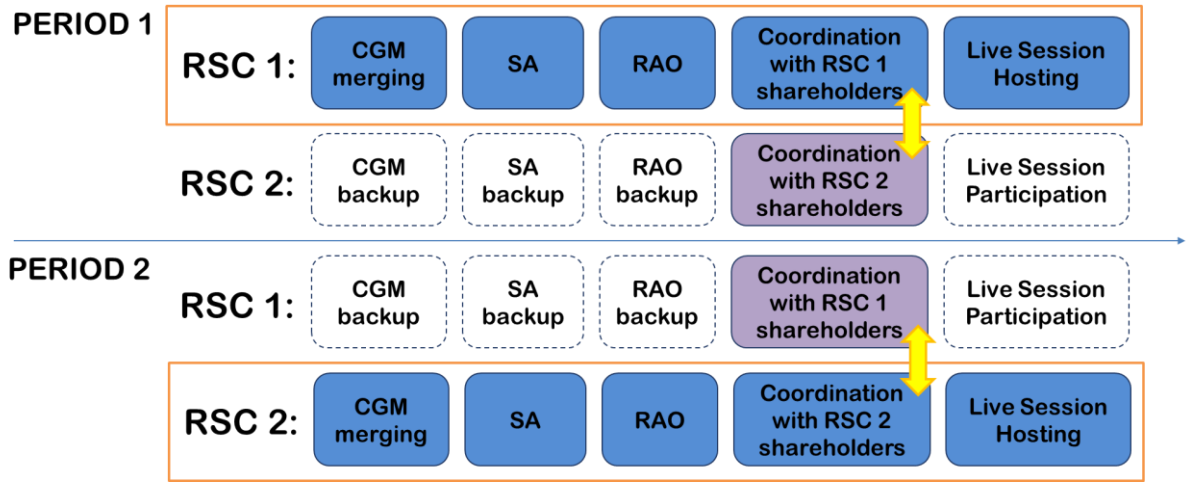
6.2 Allocation of tasks between RSCs

Article 42 is describing how the tasks listed in article 41 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) RSCs carry out a task on a rotational/alternating basis, while both (all) RSCs have a role in the process at each rotation period. The Leading RSC of a specific rotation period has the overall responsibility for the whole process, carries out the process and shares the output with the other RSC(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 RSC contributes with its expertise to support the Leading RSC, whenever needed. The Backup RSC has the overall responsibility to act as a redundant RSC for the Leading RSC whenever needed.

Example of the Rotational Model applied on CSA process:



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

- Leading RSC:
  - 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 RSC:
  - facilitates coordination with the TSOs that are non-shareholders of the Leading RSC; each TSO maintains their contact with their RSC;
  - supports the Leading RSC in the design and proposal of sets of RA;
  - acts as redundancy to the Leading RSC in case of stressed situations on the network and inability of the Leading RSC 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 RSCs 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 RSCs 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) RSCs shall participate in the CGM building process on a rotational principle, with regular building and provision of a CGM by one main RSC and one backup RSC at all times. In addition, each RSC 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 CORE RSCs 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 43 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 RSCs.

RSCs will be faced with increased reporting obligations based on Art. 46 EMR. RSCs 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, RSCs 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. RSCs 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, RSCs 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 RSCs, covering also the requirements of Article 77.

6.4 Decision-making process and governance

Coordination decision-making processes and governance will be further defined in the High-level business solution defined Article 40(4)(a) which details the cooperation between RSCs and the contractual framework between CORE RSCs and TSOs.

APPENDIX 1: EFFICIENCY AND EFFECTIVENESS ASSESSMENT

Common provisions concerning the organisation of regional operational security coordination

Efficiency and Effectiveness Assessment

3 December 2019

1. EXECUTIVE SUMMARY

The RSCs have carried out an assessment of the efficiency and effectiveness of 3 likely operating models for allocation of tasks between RSCs: Rotational, Fully Rotational and Splitting Tasks. This assessment was carried against 4 key criteria: resourcing and high-level cost assessment, expertise, resilience and business change.

Rotational Operating Model: 2 (or more) RSCs carry out a task on a rotational/alternating basis, while both (all) RSCs have a role in the process at each rotation period. Leading RSC of a specific rotation period has the overall responsibility and liability for the whole process, Backup RSC contributes with its expertise to support the Leading RSC, for the parts of the process that require specific expertise on each TSO's grid and/or coordination/communication with the TSOs, and acts as redundancy to the Leading RSC in case of stressed situations on the network and/or inability of the Leading RSC in executing the process.

Fully Rotational Model: 2 (or more) RSCs carry out a task on a rotational/alternating basis. Each RSC carries out the task in full scope for a predetermined period, after which the RSC carrying out the task changes.

Splitting Tasks: for each of the tasks listed in SOGL article 77(3), one RSC carries out a task in full scope for all timeframes without support or backup from another RSC. Different tasks can be carried out by different RSCs, in which case the tasks are split between RSCs.

Advantages of the Rotational Operating Model

The significant advantages of the Rotational Model compared to other models are the following:

- **Resilience:** continuous backup by the Backup RSC ensures business continuity, minimises/avoids delays in the CSA process in case the Lead RSC process fails; Backup RSC role reduces the risks of miscommunication and lack of coordination in case of stressed situations
- **Resourcing and high-level cost assessment**: common IT solutions of RSCs provide significant savings in the development phase and reduce the operational costs of the IT solutions.
- **Expertise:** RSCs need less time compared to other models to build and maintain expertise on the TSOs power network and operational rules that is required to fulfil the obligation of designing and optimising sets of RAs, which will provide a significant saving on the training costs
- **Business change:** smooth transition towards the target model optimises the expertise needed, reduces the implementation risks and increases the transparency, saving cost both in the development stage and in operation.

2. INTRODUCTION. HIGH LEVEL EXPLANATION OF OPERATING MODELS

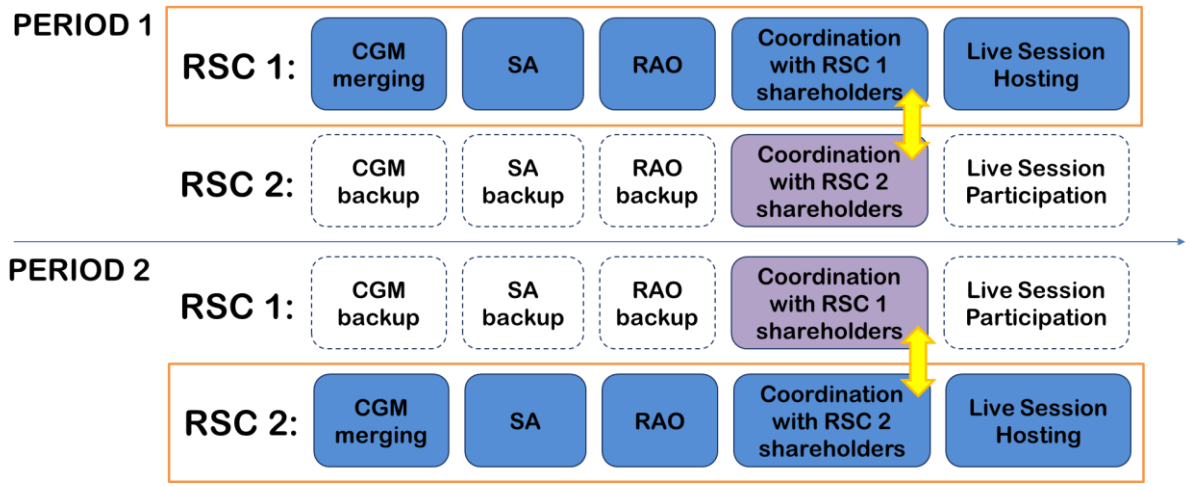
SOGL article 77(1)(c) requires that the proposals developed in each CCR include also *'an assessment demonstrating that the proposed setup of regional security coordinators and allocation of tasks is efficient, effective and consistent with the regional coordinated capacity calculation established pursuant to Articles 20 and 21 of Regulation (EU) 2015/1222'*.

There are several possible operating models; after initial analysis models based on parallel operation were excluded from the assessment because due to the overlapping implementation timelines compliance with CEP is recommended for the choice of operating model. The RSCs have carried out an assessment of the efficiency and effectiveness of 3 likely operating models for allocation of tasks between RSCs: Rotational, Fully Rotational and Splitting Tasks.

Rotational Operating Model

In case of the **Rotational Operating Model**, two (or more) RSCs carry out a task on a rotational/alternating basis, while both (all) RSCs have a role in the process at each rotation period. The Leading RSC of a specific rotation period has the overall responsibility for the whole process, carries out the process and shares the output with the other RSC(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 RSC contributes with its expertise to support the Leading RSC, whenever needed. The Backup RSC has the overall responsibility to act as a redundant RSC for the Leading RSC whenever needed.

Example of the Rotational Model applied on CSA process:



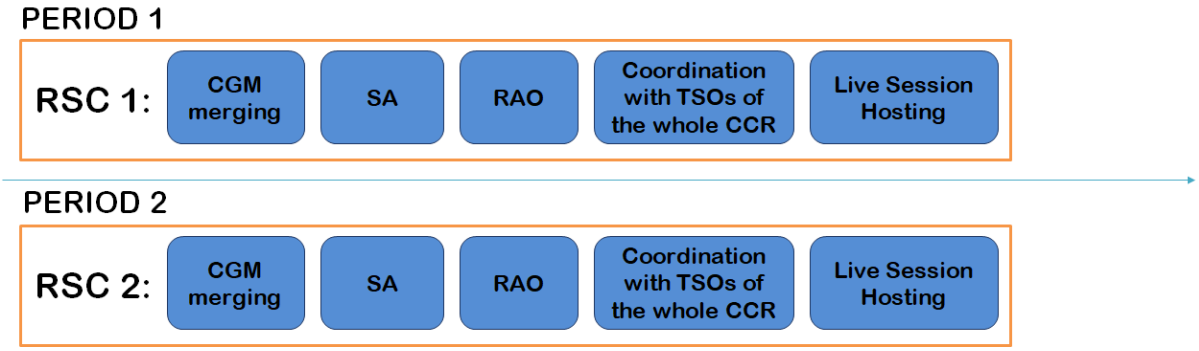
The roles and the responsibilities of the Leading and Backup RSC are the following:

- Leading RSC:
  - 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 RSC:
  - facilitates coordination with the TSOs that are non-shareholders of the Leading RSC; each TSO maintains their contact with their RSC;
  - supports the Leading RSC in the design and proposal of sets of RA;
  - acts as redundancy to the Leading RSC in case of stressed situations on the network and inability of the Leading RSC in executing the process.

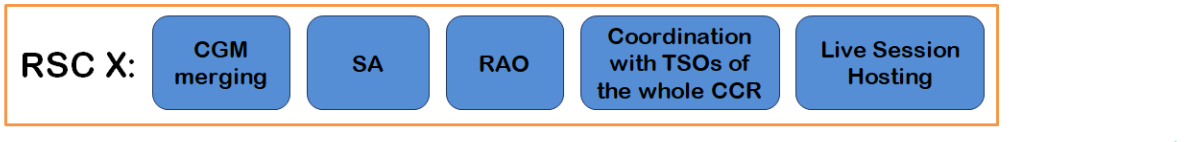
The proposed setup is consistent with the capacity calculation process. For consistency, the RSCs may rotate the CSA task on a predetermined period, but this is subject for future definition in a contractual framework.
The advantage of the Rotational Model with Leading RSC is that it is also in line with CEP requirements, meaning that no major changes in the process will be required for the proposal of establishment of RCCs due in June 2020.

Fully Rotational Operating Model

In case of the **Fully Rotational Operating Model**, two (or more) RSCs carry out a task on a rotational/alternating basis. Each RSC carries out the task in full scope for a predetermined period, after which the RSC carrying out the task changes.
Example of the Fully Rotational Model applied on CSA process:



Splitting Tasks



In case of Splitting Tasks, for each of the tasks listed in SOGL article 77(3), one RSC carries out a task in full scope for all timeframes without support or backup from another RSC. Different tasks can be carried out by different RSCs, in which case the tasks are split between RSCs.

3. COMPARISON OF THE OPERATING MODELS

High-level benchmarking table below provides a summary of the assessment that was carried out for each operating model against several criteria: redundancy/backup ensured, efficiency, effectiveness, consistency with CCC and other services, effective coordination and decision-making process, expertise, relations with non-stakeholders, compliance with CEP and costs.

	Fully Parallel	Parallel with different perimeter	Fully Rotational	Rotational	Splitting Tasks
Description	*Both RSCs carry out the task for the whole CCR*	*Each RSC carries out the task for part of the CCR*	*One RSC carries out the task for all TSOs alternating with another RSC over time*	*One RSC carries out the task alternating and with support of another RSC for expertise*	*Only one RSC is appointed for the task in a CCR*
Redundancy/ backup ensured	✓	?	?	✓	✗
Efficiency	✗	✓	?	?	✓
Effectiveness	✓	?	?	✓	✓
Consistency with CCC	✗	✗	✓	✓	✓
Consistency with other services	✗	✗	✓	?	✗
Effective coordination and decision making	?	?	?	✓	✓
Expertise	✗	✓	✗	✓	✗
Relations with non-stakeholders	?	✓	✗	✓	✗
Compliance with CEP	✗	✗	✓	✓	✓
Cost	✗	✗	?	?	?

✓ marks compliance with a criterion

✗ marks non-compliance with a criterion

? shows that further assessment is required to determine compliance with a criterion

It should be noted that the Parallel Operating Models are included in the comparison for reference; these models are considered rejected because significantly higher resources would be required, and these models are not compliant with CEP.
In the following chapters the 3 operating models – Rotational, Fully Rotational and Splitting tasks – are benchmarked against the key criteria.

3.1 Resourcing and high-level cost assessment

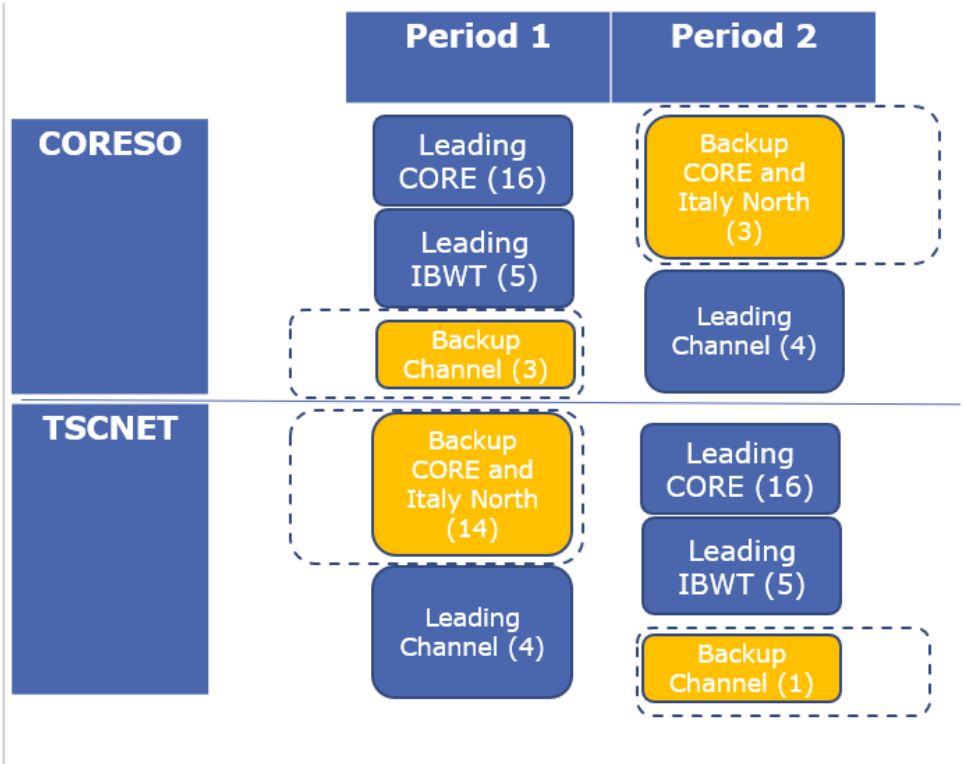
The key costs for RSCs are related to operational staff and IT tooling. **From the resourcing perspective, the Fully Rotational and the Rotational models present clear advantages.**

These operating models foresee only one RSC leading a task in a CCR at any given timeframe. In case of Rotational Model, only the Leading RSC will be responsible and accountable for the correct execution of the process and have dedicated resources to execute the task. The Backup RSC may share the workload of the Backup role between different regions.

The Rotational model would require 5 desks in 2 RSCs to cover the processes in 3 regions compared to 3 desks in case of the Fully Rotational Model or Splitting Tasks, but it ensures continuous backup that would not be there in case of the other 2 models. It is also important to note that since the implementation of the CSA service in full scope will be a major business change, Rotational Model is the only model that would allow a smooth transition optimising the expertise needed, saving cost both in the development stage and in operation.

The second significant component of costs is related to IT tools. In case of the Rotational Model the RSCs would share common IT solutions, providing significant savings in the development phase and reducing the operational costs of the IT solutions. It is also important to note that in addition, common IT solutions ensure transparency and facilitate the fulfilment of reporting obligations.

Operational arrangement with Rotational Model

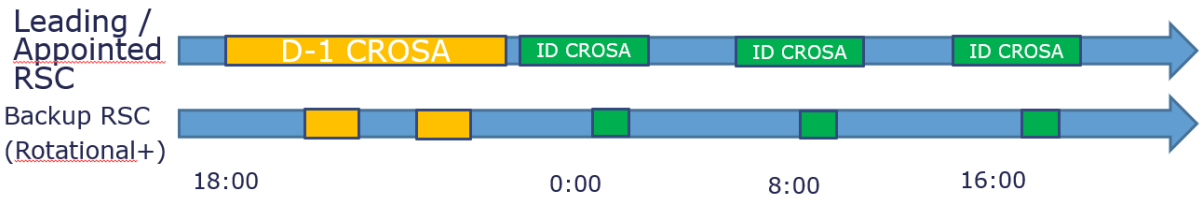


Shows potential combinations of backup desks with other regions (for example Channel backup and SWE). In (), the number of TSOs participating to the ROSC.

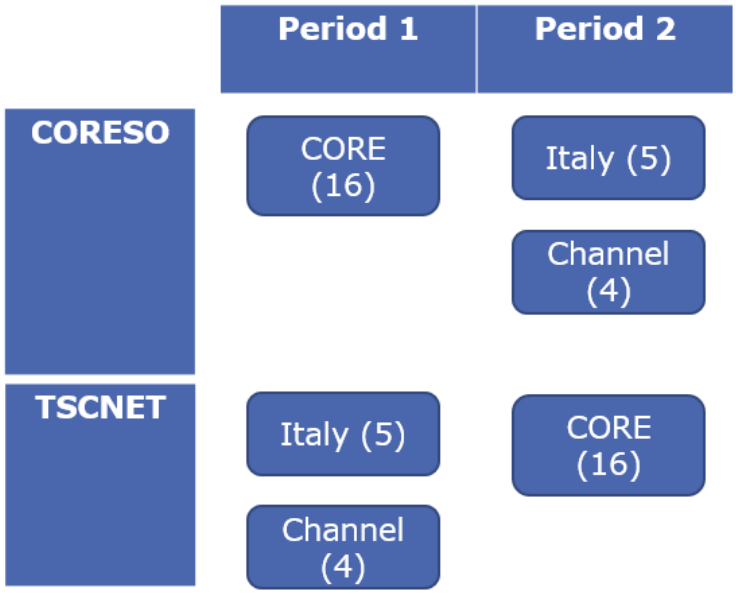
As shown above, the Leading RSC has one dedicated desk for each region that it is leading, for example CORE Lead has one desk dedicated to CORE CCR, Italy North Lead has one desk dedicated to Italy North CCR, while the Backup RSC has one desk for the backup function with the possibility to combine this backup desk also with other regions.

The advantages of this setup are resilience/security, optimal use of expertise and smooth change, as further elaborated in chapters 3.2-3.4. The expected higher need for the number of desks across 2 RSCs is well balanced by ensuring business continuity through continuous backup. Continuous backup will allow the Backup RSC to take over running the process in case the Lead RSC fails with minimal or no delays in the process.

The workload per desk in one RSC in the Rotational Model in day ahead and intraday timeframe is shown below:

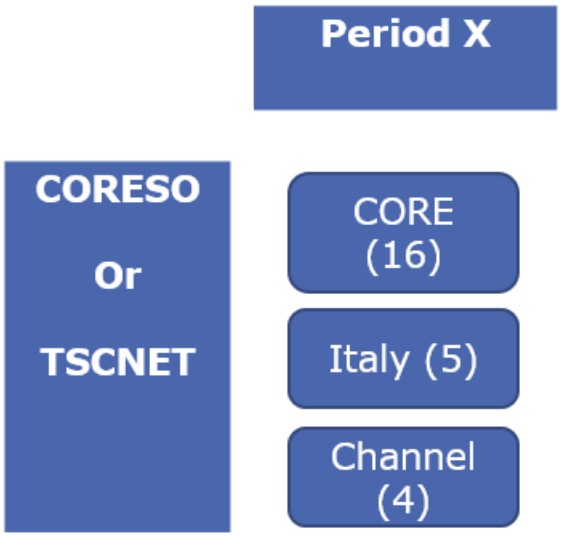


Operational arrangement with Fully Rotational Model



The advantage of the setup is that only 3 desks will be required across 2 RSCs, while the disadvantages are: no immediate backup, high workload for one RSC and RSCs need to build expertise on the whole CCR.

Operational arrangement if RSCs split tasks



The disadvantages for the setup are massive change required in each RSC (reallocation of resources, building expertise), no backup ensured and the risk of lack of transparency and discriminatory behaviour (1 RSC runs the service for all TSOs « forever »).

3.2 Expertise

The CSAm requires RSCs to analyse, design and propose sets of Remedial Actions. This can be only done when an adequate level of expertise is kept at the RSC level. Furthermore, the Clean Energy Package requires that there is an official training and certification process for RCC personnel.

All of the 4 RSC tasks defined in SOGL require that the RSC has expertise on the TSOs power network and operational rules. This is necessary to fulfil the RSC role of designing and optimising sets of RA and also to develop and improve the RAO, among other roles, and will be required even with a high level of automation for the target process. The Fully Rotational or the Splitting Tasks models would require that one RSC has all the network and operational expertise for one region.

Taking the above into account, it is more expensive and riskier for a RSC to build up expertise and achieve a high level of maturity in the operational relations for the whole CCR, giving a clear advantage to the Rotational Model.

To achieve the level of expertise required to perform all the tasks, most notably to be able to analyse the results of security assessment, design and propose remedial actions, each operator will have to follow a training plan consisting of at least (i) a theoretical training on each TSO's power network and operating rules, and the procedures in each region, (ii) a practical training in the RSC control room working in parallel with an instructor, and, ideally (iii) a practical training in the control room of each TSO to further improve the understanding about each TSO's grid.

Based on a rough estimation and an assumption that both RSCs follow the same training plan, the table below gives an indication of the total time required to train one new operator to perform the tasks in case of each operating model.

	ROTATIONAL		**FULLY ROTATIONAL**	**SPLITTING TASKS**
Number of TSOs for which expertise is required	*CORESO*	*TSCNET*		
CORE	*3*	*14*	*16*	*16*[2]
Italy North	*2*	*3*	*5*	*5*
Channel	*3 + ICs*	*1 + ICs*	*4 + ICs*	*4 + ICs*
Initial training	CORESO	TSCNET		
CORE	4 months	15 months	18 months	18 months
Italy North	3 months	2 months	5 months	5 months
Channel	4 months	1 month	5 months	5 months
Time required to maintain expertise	CORESO	TSCNET		
CORE	5 days/year	21 days/year	26 days/year	26 days/year
Italy North	3 days/year	5 days/year	8 days/year	8 days/year
Channel	6 days/year	3 day/year	8 days/year	8 days/year

As seen in the table, the Rotational model will require less time both for initial training of the new operators, as well as for maintaining the expertise through continuous training.

[2] In the Core Region 50Hertz is counted on TSCnet and Coreso side, due to their participation in both RSCs.

Considering the notable staff turnover in the RSC control rooms, due to the conditions of secondment from TSOs and natural career evolution, the reduced time required for both initial and continuous training would provide a significant saving on the training costs.

3.3 Resilience

Ensuring security of supply requires that one RSC is available at all times, 24/7, to provide the coordination services to TSOs. In order to ensure this, a redundancy to the RSC that is executing the tasks is essential. The Fully Rotational and the Splitting Tasks operating models do not ensure redundancy. The Rotational Model ensures that there are RSC coordination rooms focused on the European network 24/7 so that there is full readiness to deal with critical grid situations, IT failures and other force majeure situations. With a Leading RSC and with a Backup RSC, there are also faster response times given the higher level of availability.

The communication and coordination between RSCs and TSOs are essential and, in case of stressed situations, the workload in the RSC's control rooms is very high, increasing the risk of miscommunication or even lack of coordination. There is a high number of stakeholders participating to in the CSA process that justify a structured coordination between RSCs and TSOs, and not only multiple TSOs to one RSC. **In case of the Rotational Model the Backup RSC can significantly reduce the risks mentioned above by supporting the Lead RSC with communication and coordination with its shareholder TSOs.**

In the last decade there is a notable increase of operational risks due to increase of intermittent generation, increased capacity and variability of flows in the European network. The fact that no extensive or wide area incidents have been recorded in the interconnected European electricity network since the establishment of RSCs in 2009 is the best indicator of the effectiveness of the regional coordination.

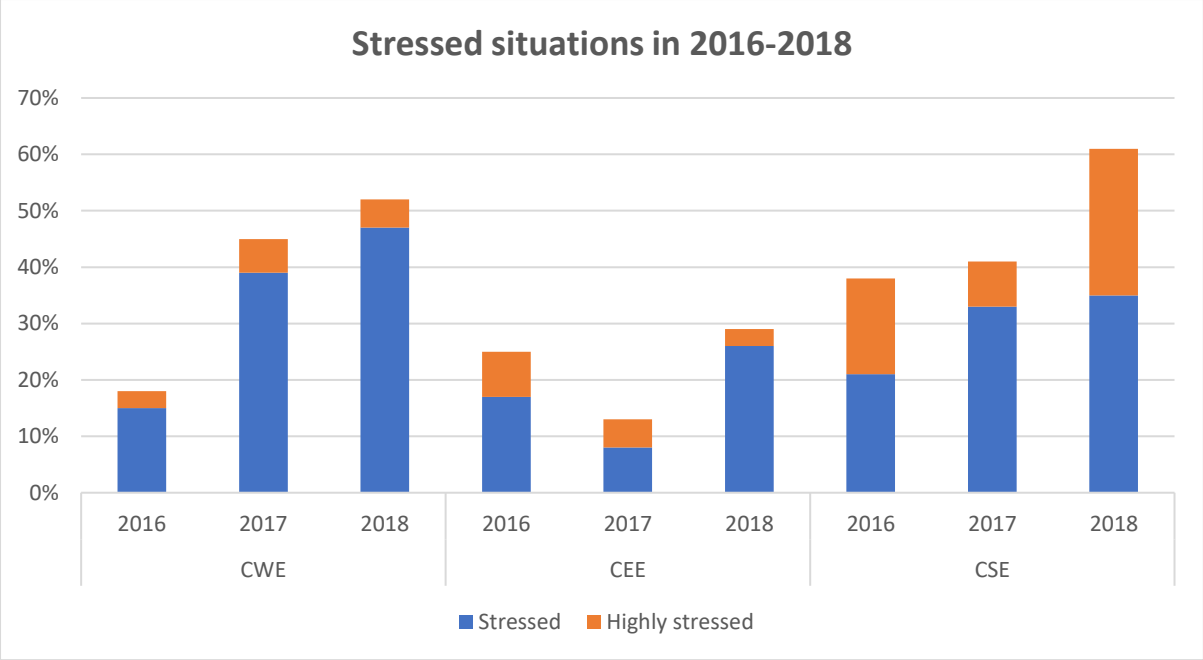
ENTSO-E annual reports on Incident Classification Scale[3] show that since the beginning of reporting in 2013 no blackouts (classified as scale 3 incidents according to the Incident Classification Scale) have occurred in any of the synchronous areas, and only a limited number of extensive incidents (classified as scale 2 incidents), when a TSO is in emergency state, have occurred, mainly in isolated systems of Iceland and Cyprus, where the SOGL requirements on regional coordination do not apply. Notable scale 2 incidents outside isolated systems were three N-violations (overloads on transmission lines classified as scale 2 incidents) in 2018 reported in Continental Europe, which were caused by unexpected high flows on the Switzerland and Italian border due to unexpected high production in Italy demonstrating further how crucial is the need for effective coordination in case of stressed situations.

CORESO Yearly Operational Reviews[4] show that the number stressed situations has been increasing in most regions, for example in 2018 in South Central Europe (Italy North region) there were stressed situations in 61% of the business dates.

In case of stressed situations and/or when a TSO rejects a remedial action, the remedial action coordination step in the CSA process (between timings T1 and T2 in the 1st coordination run and between T3 and T4 in the 2nd coordination run) becomes more challenging, the number interactions between RSC and TSOs increase – on average there are 6 interactions (e.g. phone calls, e-mails) between a RSC and a TSO in such stressed situations. **In case of the Rotational Model these RSC-TSO interactions are divided between the RSCs, improving the quality of the services and reducing the risks of delay in the process.**

[3] ENTSO-E reporting on Incident Classification Scale starting from 2017 (SOGL compliant) is available here - https://www.entsoe.eu/network_codes/sys-ops/annual-reports/#incident-classification-scale, earlier reports covering the years 2013-2016 are available here - https://www.entsoe.eu/publications/system-operations-reports/#steering-group-operations

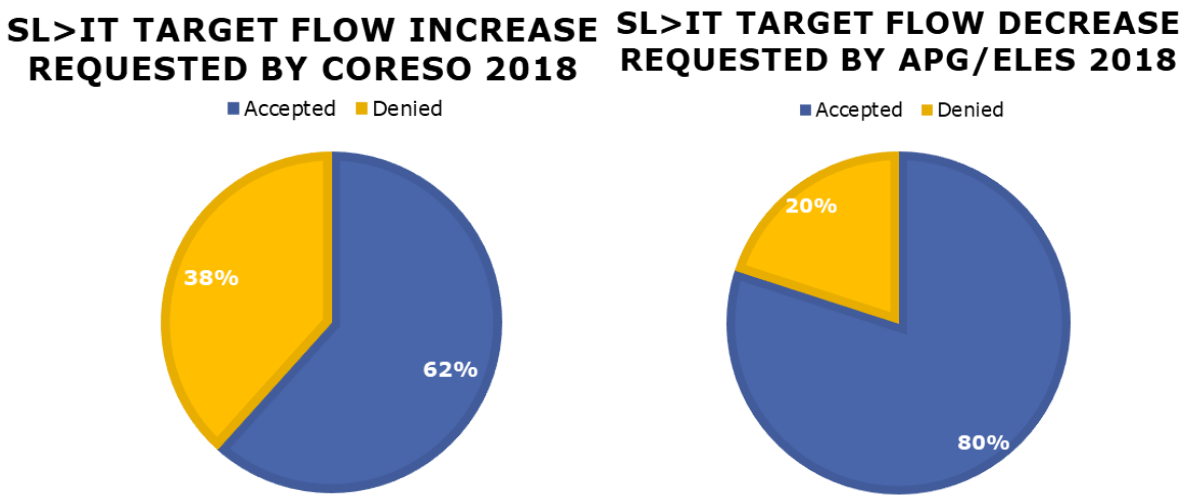
[4] Coreso Yearly Operational Reviews are available on Coreso website - https://www.coreso.eu/operational-data/operational-review-2/



It is also important to note that often the interactions are multilateral including several TSOs in order to propose an acceptable set of remedial actions. The estimated total number of interactions between Coreso and TSOs during D-1 studies in case of data quality issues or conflicting remedial actions is **4745 interactions per year**.

	CORE (CWE+CEE)	**IBWT**
Number of days with coordinated actions	190 (52%)	222 (61%)
Estimated number of coordinated RAs	**950 RAs (2018)**	**1110 RAs (2018)**
Number of days with rejected RA	TBD	213 (58%)
Estimated amount of cross-border RDCT avoided with the proposed coordinated RAs	TBD	**15 GW**

The graphs below illustrate the proportion between accepted and rejected RAs in the Italy North region in 2018 – sets of remedial actions proposed by TSOs have been rejected in more than 73 business dates, and RAs proposed by RSCs have been rejected on 140 business occasions.



The coordination step can be supported by an IT solution (such as the Coordination Function) but it cannot be automated, especially in case of stressed situations and in case remedial actions proposed by RSC/RAO have been refused by a TSO. In addition, on the way to a fully automatized remedial action optimisation, while RAO tools are being developed and in a transition phase, RAO results may have to be challenged by an operator.

In case of the Rotational Model the Backup RSC can support the Lead RSC in the coordination step with the interactions with TSOs, finding alternative RA proposals in case of refusals by TSOs, challenging the results of RAO and also supporting in case of failures of the RAO tool. Based on the current experience, without the support of the backup RSC, it is unlikely that one RSC can complete the process in a timely manner. Especially in case of stressed situations there would be delays in the process that will affect all CCRs.

Also, the Rotational Model ensures that the relation between the Leading RSC and the non-shareholder TSOs will be efficient without the need for building trust and new operational relations. In case of the other models – Fully Rotational and Splitting Tasks – building relations between one RSC and non-shareholder TSOs will require time-consuming discussions around operational processes, contracts and operational interactions overall, which would be challenging or maybe even not feasible considering the current expectations of NRAs regarding the implementation timeframe.

Regarding decision-making, the concept of one Leading RSC adequately supported by a Backup RSC provides a robust decision-making process between the RSC and the remedial action owner (TSO). The complexity of the network, the intermittent generation and the number of parties involved result in risks for the security of the network that are more difficult to address when increasing the distance between the remedial action owner (TSO implementing the RA) and the decision-making stakeholders.

3.4 Business change

Implementation of the CSA process will require development of several tools (RAO, Coordination Function, CSA Input Consistency Function, etc), establishment of the operational processes, introducing a link with other processes (STA, OPC, CCC), with other regions, etc. This is without a doubt a challenging undertaking, causing a huge change for both TSOs and RSCs. Considering this, it would be more reasonable to introduce the change in operational processes step-by-step, taking the maximum of the already existing processes and expertise, instead of making a dramatic change of all the processes/tools all at once. Implicitly, smoother change in the processes will minimise the impact on the security of supply.

The Rotational Model allows for a pragmatic and agile approach to the implementation, the already existing expertise and experience with the already established processes would be used most efficiently. The Rotational Model also prepares the RSCs and TSOs for the CEP implementation without creating new risks in the operational processes.

It is also important to note that implementation of other services already foresees huge change for TSOs and RSCs. Looking at the experience with other major projects, for example CGM Project, such step-by-step approach might be the only way to avoid critical delays in implementing the CSA process.

Main advantages of the Rotational Model:

- **Reduction of implementation risks**: minimising the magnitude of change over a time period will also minimise costs for RSCs and TSOs, dividing the total costs over a longer period of time, as well as ensuring that the costs borne are justified and contribute towards the end target (reducing also the risks related to managing the budget in case of scope changes), as well as minimising the risk for delays in the overall implementation project
- **Transparency:** through the Rotational Model, with both RSCs involved in the effective regional operational security coordination, the interoperability of tools and processes in one region and between different regions will be ensured. This will reassure that RSCs report on behalf of all TSOs and reinforce transparency and neutrality for the European consumer.

Main advantages of Splitting Tasks:

- **Effectiveness:** for the processes which are perceived not as critical to maintain a backup entity within the Region, the splitting of tasks allows the RSCs to focus their resources on less number of processes and at the same time increases their efficiency in terms of operational staff to be trained as well as the maintenance of IT tools and resources.

The Rotational model for time critical processes of high availability, including a Leading RSC and a Backup RSC, ensures an efficient and effective regional operational security coordination and allows for the correct, safe and timely execution of RSC tasks. While splitting the tasks for processes which are not as critical in terms of impact and timings, would be the most efficient way regarding staffing and IT resources.

It is also important to note that RSCs will annually 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 RSCs, covering also the requirements of Article 77. These assessments will allow to identify possible inefficiencies early on.