Explanatory note to the South West Europe TSOs proposal 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 electricity transmission system operation

October 2019

Version for Public Consultation

Disclaimer: This explanatory document is submitted by the TSOs of the South West Europe region for information and clarification purposes only accompanying the TSOs' proposal 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 electricity transmission system operation.

Table of contents

Table of figures

1 Introduction

This technical document sets out the main principles for the proposal for regional operational security coordination applied in South West Europe (SWE) region. These principles shall be applied by all TSOs of SWE region and the regional security coordinator of SWE region

The participating TSOs for this proposals are REE (SP), REN (PT) and RTE (FR). The following borders are considered: Spain – France and Spain – Portugal.

This proposal is necessarily compatible with the methodology for coordinating operational security analysis developed in accordance with Article 75 of Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation and with the methodologies developed in accordance with Articles 35 and 74 of Commission Regulation (EU) 2015/1222 of 24 July 2015 establishing a guideline on capacity allocation and congestion management.

2 Definitions and acronyms

a. 'SO regulation' means Electricity Transmission System Operation Guideline according to Commission Regulation (EU) 2017/1485.

b. 'CACM regulation' means Capacity Allocation and Congestion Management Guideline according to Commission Regulation (EU) 2015/1222.

c. 'CSA Methodology' means Methodology for coordinating operational security analysis in accordance with Article 75 of Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation.

d. 'IGM' means Individual Grid Model.

e. 'CGM' means Common Grid Model.

f. 'PST' means phase shifter transformer.

g. 'RSC' means regional security coordinator.

h. 'CNE' means critical network element.

i. 'SPS' means special protection scheme. SPS are automatically or with manual approval executed to sustain a stable and secure system state after the occurrence of contingencies. SPS are a possible application for curative remedial actions.

j. 'XRA' means a remedial action identified as cross-border relevant and needs to be applied in a coordinated way.

k. 'RAO' means remedial action optimizer.

3 Appointment of the regional security coordinator

According to Article 77 of SO Regulation, this proposal shall include the appointment of the regional security coordinator. All TSOs from SWE agree to designate CORESO as SWE RSC to perform regional operational security coordination.

In executing this task, the SWE RSC will have to carry out all the needed studies to perform the regional operation security analysis. The SWE RSC will report all the identified constraints to SWE TSOs in those cases, the SWE RSC will have to identify the most effective and economically efficient remedial action. The SWE RSC will have to exchange all needed information with SWE TSOs to agree on the remedial actions.

4 Day ahead coordinated security analysis

SWE RSC will have to perform the day ahead coordinated security analysis.

All requirements established in Article 23 of the CSA Methodology will be respected.

The results of each study will cover the 24 hours of the day beginning at 00:00.

According to article 23.4 of the CSA Methodology, all TSOs of a CCR have the right to establish particular rules applicable in day-ahead to the CSA and CROSA performed by the RSC. By the configuration of the Spanish French border as a peninsula, the impacts of frequency adjustments for the peninsula are concentrated on one border (FR-ES), leading to important variations of electricity flows. To fulfil RTE regulation that does not allow overflows due to unintended deviations of frequency adjustments, the exchange shall be increased of 200MW during the study of the coordinated security analysis performed by the SWE RSC for the French-Spanish border. This increase of exchange during the study aims to cover the unintended deviations of physical electricity flows caused by the adjustment of electricity flows to maintain a constant frequency, and then to make sure that these unintended deviations will not lead to emergency states in real time.

5 Intraday regional coordinated security analysis

The intraday coordinated security analysis shall be performed by the SWE RSC. The process shall respect the article 24 of the CSA Methodology

These intraday analysis will take into account the latest available information including updated renewable energy sources and load forecasts, market positions, last technical information on network availability, remedial actions availability. With all this information it will be possible to reassess the previously agreed remedial actions not yet activated to find if it is still needed of whether any other remedial action is more efficient.

A minimum of three coordinated security analysis per day shall be processed for the following ”reference hours” :

- At 00:00 to have a first overview for the coming daytime, and to take into account the preventive remedial actions from the day ahead coordinated regional security analysis.
- At 08:00 to have the updates and more accurate load and generation values, especially for the renewable energies.
- At 16:00 to have more accurate data to study the afternoon, and the latest load variations (load peak of the afternoon).

- And on request from a SWE TSO if needed. The reasons to ask for an additional coordinated security analysis could be: a change of forecasts, an important change of topology, an extreme event, etc.

According to CGMM one hour before the reference hour the information needed to create the CGM will be available. When no incident appears, the intraday process will begin 45 minutes before the reference hour and will finish 45 minutes after the reference hour including the final validation, as shown in Figure 1.

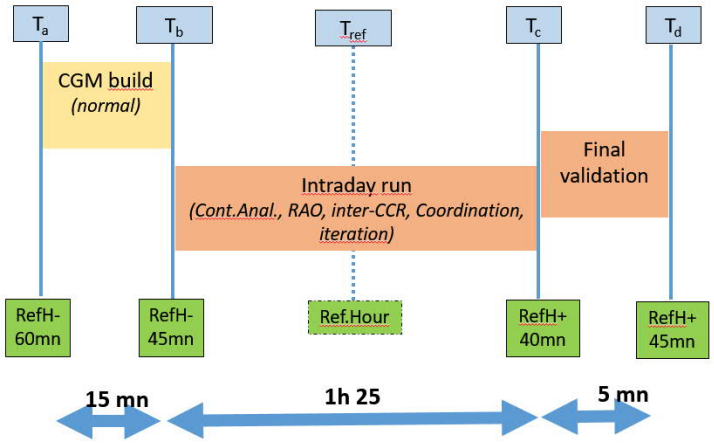

Figure 1 Intraday regional coordinated security analysis process

The results of each study will cover from two hours after the reference hour until the end of the day.

According to article 24.6 of the CSA Methodology, all TSOs of a CCR have the right to establish particular rules applicable in intraday to the CSA and CROSA performed by the RSC. By the configuration of the Spanish French border as a peninsula, the impacts of frequency adjustments for the peninsula are concentrated on one border (FR-ES), leading to important variations of electricity flows. To fulfil RTE regulation that do not allow overflows due to unintended deviations of frequency adjustments, the exchange shall be increased of 200MW during the studies of the coordinated security analysis performed by the SWE RSC for the French-Spanish border. This increase of exchange during the studies aims to cover the unintended deviations of physical electricity flows caused by the adjustment of electricity flows to maintain a constant frequency, and then to make sure that these unintended deviations will not lead to emergency states in real time.

5.1 Coordinated operational security analysis “on request”

When a SWE TSO faces a situation in which a new regional coordinated security analysis is needed, he will be able to ask for an additional study called “on request”. In this case, the SWE TSO asking for the security analysis “on request” will have to update his files including the new situation that caused the need for a new study. The others SWE TSOs will not have to update their files. Therefore SWE RSC

will merge the new files from the TSO asking for the "on request" security analysis with the latest updates of the others SWE TSOs files in order to perform the analysis.

The SWE TSO asking for an additional security analysis shall precise to the SWE RSC and the others SWE TSOs the reasons that cause the need for a new study and the scope thereof, hence the SWE TSO shall clarify if the analysis is needed for all the borders or not, and for all the remaining timestamps or just some specific ones to be specified by the TSO.

If the requested additional security analysis is asked for all the timestamps it will be called a "complete CSA on request" in the rest of the document. If not it will be called a "light CSA on request"

If a CSA on request is requested in the period where the previous defined CSA is running, the SWE RSC shall always finish the ongoing security analysis, except if the additional requested security analysis is due to erroneous data sent at the previous planned timestamp that could be possibly impacting for the results. The SWE RSC shall then abort the study for the impacted border with the erroneous data and finish it for the non-impacted border before performing the requested CSA. The above mentioned approach can be admissible due to the fact that there is independence between borders in SWE CCR.

If a "complete CSA on request" is requested in the period where no defined CSA is running, the SWE RSC shall perform it only if it is asked for more than 90 minutes before the next defined CSA.

In case of a "light CSA on request" is requested in the period where no defined CSA is running, the SWE RSC shall perform it only if the results of the CSA are expected to be delivered prior to the SWE RSC coordination deadline and prior to the beginning of next defined CSA.

5.2 RSC coordination deadline

According to the SWE RDCT methodology the RSC coordination deadline must be defined in this proposal, it is agreed that deadline for the coordination of RSC is one hour.

5.3 Fast activation process

A fast activation process shall be considered if the RSC coordination deadline has been exceeded without any recommendation by the SWE RSC or if any SWE TSO detects an identified constraint after RSC Coordination Deadline, when there is no time left to perform a coordinated security analysis on request and to apply its relative remedial actions. In that case, the TSO who has detected the identified constraint shall contact the other concerned TSOs if they are affected by any consequences of the identified constraint or by any remedial action identified to be applied to solve the constraint.

If the remedial action proposed shall be activated by the other TSOs, the TSO detecting the identified constraint shall ensure that the remedial action is accepted. Both TSOs shall inform each other of the different remedial action activations steps.

Once the system is stabilized, the TSO concerned by the identified constraint shall inform the SWE RSC of the situation and all the remedial actions applied.

6 Preparation of Remedial Actions

6.1 Procedure for exchanging relevant information

To carry out the regional operational security analysis it is necessary to exchange a significant volume of information between SWE TSOs and SWE RSC.

SWE RSC will need operational security limits for the elements of the transmission network of all SWE TSOs. SWE RSC will also need the complete contingency list of all SWE TSOs.

SWE TSOs shall send SWE RSC the list of grid elements that must be monitored to detect the possible violations of security limits. The list of these secured elements will have to be sent before each regional operational security analysis during intraday and D-1. It has been agreed by all SWE TSOs that the list of secured elements must include, at least, the critical network elements of SWE.

To propose the most effective and economically efficient remedial actions, SWE RSC need to have information about the availability, volume and price of the remedial actions, for that reason SWE TSOs shall send these data sent before each regional operational security analysis during intraday and D-1. It has been agreed by all SWE TSOs that the list of proposed remedial actions must include, at least, the remedial actions proposed for the capacity calculation process. In the same way SWE RSC must be informed if the status of availability of a remedial action that had been previously agreed change. In those situations the relevant TSO shall inform SWE RSC and also the others SWE TSOs of this circumstance and explain the technical reasons that have resulted in this unavailability

6.2 Determination of cross-border relevant remedial actions

To assess the cross border relevance of remedial actions, each SWE TSO shall first assess its remedial actions qualitatively. This assessment shall then be shared by the border country/countries among SWE CCR. The other TSO(s) shall also give its/their qualitative assessment on the other TSO remedial actions. For the remedial actions with disagreement, the influence factor shall be calculated by the TSO which proposes the remedial action, based on the adequate situations in accordance with the Art.15 of CSA Methodology. In these cases, all SWE TSOs agree that the threshold for the remedial action influence factor is 5%.

For the sets of remedial actions, as too many possible combinations are possible and the optimizer results cannot be anticipated, all SWE TSOs agree to consider a set of remedial actions cross border relevant if one of the remedial actions in the set has been assessed as cross border relevant.

To ensure that the result of this evaluation is appropriate, all SWE TSOs agree that the determination of cross- border impacting relevant remedial actions must be assessed every year and in case of a new remedial action proposed.

6.3 Identification of most effective and economically efficient remedial actions

During coordinated operational security analysis, where SWE RSC identifies a constraint, it shall recommend the most effective and economically efficient remedial action or set of remedial actions to relieve all violations of security limits. These recommended remedial actions can be different from those proposed by SWE TSOs, SWE RSC shall include explanations for this decision.

To recommend the most effective and economically efficient remedial action or set of remedial actions, SWE RSC will develop and use a Remedial Action Optimizer to monitor power-flows, voltage and angle difference. In an initial phase it will only monitor power-flows. Computations will start from the common grid models.

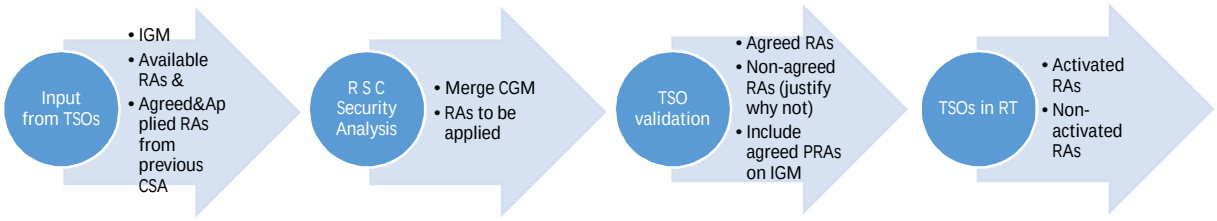

Figure 2 Coordinated security analysis process

7 Validation

7.1 Day ahead validation

The day ahead validation procedure shall take into account the hours included in Article 33 of CSA Methodology.

The reasons to refuse a remedial action could be the following:

- RAs are no longer available
- RAs imply additional cost on affected TSOs, not identified by the RSC study
- RAs implementation leads a system to an unsecured situation.

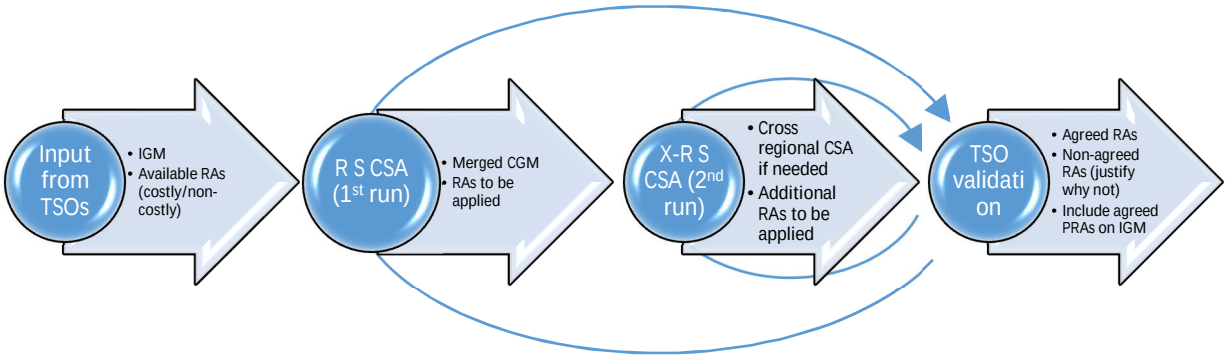

Figure 3 High level vision of the Day-Ahead process

Where violations of operational security limits remain not solved at the end of the cross-regional day-ahead coordinated operational security assessment process, the concerned SWE TSOs and SWE RSC shall agree on the objectives and the needed steps to follow in intraday in order to improve the management of these remaining violations.

During this process, SWE RSC and SWE TSOs may have additional exchanges needed to facilitate its effectiveness.

7.2 Intraday validation

In each intraday, when SWE RSC performs coordinated regional operational security assessments, it shall take the cross-regional day-ahead or last intraday coordinated operational security assessment outcomes and agreed remedial actions as a reference basis, against which needed adaptations shall be assessed. Thus, each SWE TSO shall include the agreed remedial actions in the last coordinated operational security assessment (day-ahead or last intraday) in their first intraday IGMs that will be used by SWE RSC for the next operational security assessments to be provided after T5.SWE RSC shall inform SWE TSOs of all the proposed remedial actions, during the assessment of security in each intraday, namely:

- The RA non-cross border relevant
- The RA cross border relevant.

Any remedial action proposed by a SWE TSO can be refused by this SWE TSO.

Cross border relevant remedial actions can also be refused by the XRA affected SWE TSO.

In any case the refusing SWE TSO shall give the reason and SWE RSC shall look for another RA taking into account the different SWE TSO feedbacks

The reasons to refuse a remedial action could be the following:

- RAs are no longer available
- RAs imply additional cost on affected TSOs, not identified during the RSC study
- RAs implementation leads a system to an unsecured situation.

Each SWE TSO shall apply these actions for the elements located in its control area if it is compatible with real-time conditions.

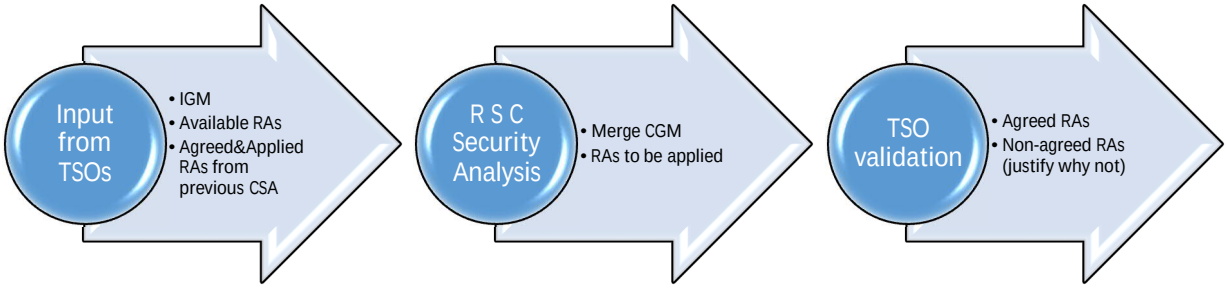

Figure 4 High level vision of the Intraday process

After the assessment of each intraday SWE RSC shall organize a session, such as a teleconference, where the results of coordinated regional operational security assessments performed and proposed remedial actions are shared. During this session, SWE TSOs and SWE RSC shall consolidate the outcomes of the whole process. Each SWE TSO shall participate to this session or shall appoint SWE RSC to represent it at the session while the SWE TSO keeps the legal responsibility to agree on each remedial action.

When violations of operational security limits remain not solved at the end of the cross-regional intraday coordinated operational security assessment process, the concerned SWE TSO and SWE RSC shall agree on the objectives and the needed steps to follow in next intraday in order to improve the management of these remaining violations.

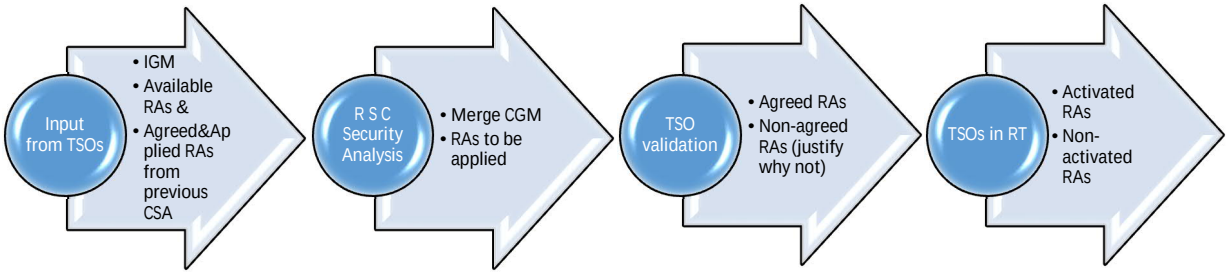

Figure 5 High level vision of the last Intraday process before Real Time

8 Timescale for the Implementation

8.1 Prerequisites

When the new Regional CSA goes live, the analysis will be performed by the SWE RSC based on input provided by the TSOs, and finally validated by the TSOs. Some crucial elements in this process are:

a. TSOs' input provision;

b. Common Grid Model (CGM);
c. Remedial Action Optimization Tool.

The implementation of this methodology is subject to the implementation of CGMES format in the CCR. CGM is not developed by the SWE CCM project, but by a coordinated project of all ENTSO-E TSOs.

The remedial action optimization tool is being developed by the SWE RSC.

All these prerequisites shall be implemented before the "go-live" of the Regional CSA.

8.2 Timeline for implementation of the CCM

The following timeline is estimated for the implementation of the process:

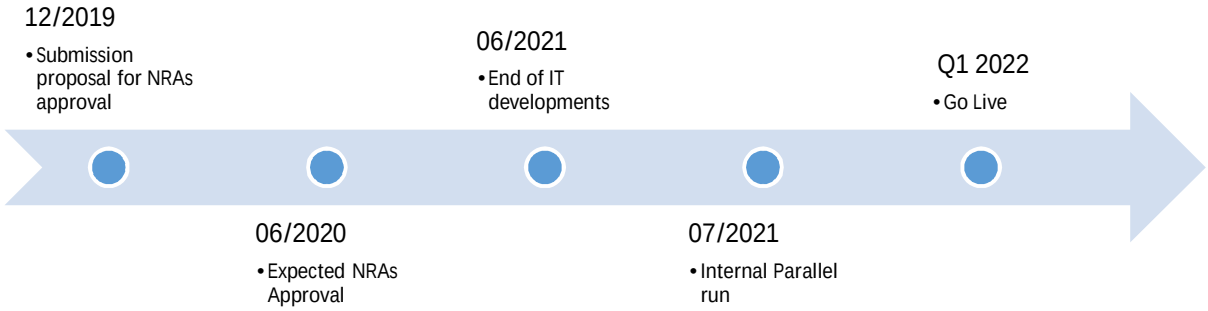

Figure 6 Implementation plan