All TSOs' of Baltic Capacity Calculation Region common provisions for regional operational security coordination in accordance with Articles 76 and 77 of the Commission Regulation (EU) 2017/1485 of 2 August 2017

19 August 2020

Table of contents

1. Introduction

Whereas

(1) This document is a Common Provisions of Baltic Capacity Calculation Region (hereafter referred to as Baltic CCR) for Regional Operational Security Coordination (hereafter referred to as Baltic ROSC) in accordance with articles 76 and 77 of Commission Regulation (EU) 2017/1485 of 2 August 2017 (hereafter referred to as the “SO Regulation”).

(2) These Common Provisions take into account general principles and goal set in SO Regulation as well as Commission Regulation (EC) 2015/1222 establishing a guideline on Capacity Allocation and Congestion Management (hereafter referred to as the “CACM Regulation”).

(3) It is necessary to standardise operational security analysis at least per synchronous area according to Article 75(1) of the SO Regulation respectively within CCR according to Article 76(1) of the SO Regulation. General standardisation principles defined in a common methodology for coordinated operational security analysis (hereafter referred to as – CSAM) according to article 75 of the SO Regulation which shall be considered as legal basis for these Common Provisions.

(4) These Common Provisions consider and where necessary complement the CSAM and where necessary, the methodologies developed in accordance with article 35 of the CACM Regulation (hereafter referred to as “CRC Methodology”) and article 74 of the CACM Regulation (hereafter referred to as “CRCCS Methodology”).

(5) Articles 76 and 77 of the SO Regulation constitute the legal basis for these Common Provisions and define several requirements that it should include at least:

a) conditions and frequency of intraday coordination of operational security analysis and updates to the common grid model by the RSC;

b) the methodology for the preparation of Remedial actions (hereafter referred to as - RAs) managed in a coordinated way, considering their cross-border relevance as determined in accordance with article 35 of CACM, taking into account the requirements in articles 20 to 23 of the SO Regulation and determining at least:

i. the procedure for exchanging the information of the available RAs between relevant TSOs and the RSC;

ii. the classification of constraints and the RAs in accordance with article 22 of the SO Regulation;

iii. the identification of the most effective and economically efficient RAs in case of operational security violations referred to in article 22 of the SO Regulation;

iv. the preparation and activation of RAs in accordance with article 23(2) of the SO Regulation;

v. the sharing of the costs of RAs referred to in article 22 of the SO Regulation, complementing, where necessary, the common methodology developed in accordance with article 74 of the CACM Regulation.

(6) In conclusion, these Common Provisions document shall contribute to the general objectives of the SO Regulation to the benefit of all TSOs, regulatory authorities and market participants.
(7) Common Provisions of Baltic ROSC may be amended and specified in the future considering the upcoming requirements from Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity.

1.1 Definitions and abbreviations

For the purposes of the Common Provisions of Baltic ROSC, the terms used in this document shall have the meaning of the definitions included in article 3 of the SO Regulation, article 2 of the CACM Regulation, article 2 of the Regulation 543/2013, article 2 of CSAM and the other items of legislation referenced therein. In addition, the following definitions shall apply:

Available remedial action - is a remedial action which is available to solve constraints. It includes the needed technical and cost information.

Baltic TSOs - the transmission system operators for electricity of the Republic of Estonia, the Republic of Latvia and the Republic of Lithuania.

Baltic RSC – Baltic regional security coordinator, which provides service for three Baltic TSOs in the following countries: the Republic of Estonia, the Republic of Latvia and the Republic of Lithuania. Baltic RSC area of operation also includes cross-borders between EE-FI, EE-LV, LV-LT, LT-SE and LT-PL.

Baltic RSC Agreement – Means Baltic regional security coordinator agreement signed by Elering, AST and Litgrid on 31 October 2016.

TSOs of Baltic CCR - the transmission system operators for electricity of the Republic of Estonia, the Republic of Finland, the Republic of Latvia, the Republic of Lithuania, the Republic of Poland and Sweden.

Baltic CCM – means Capacity calculation methodology within the Baltic Capacity Calculation region in accordance with article 20(2) of the Commission Regulation (EU) 2015/1222.

CRCCS Methodology - means the “Baltic CCR TSOs common methodology for redispatching and countertrading cost sharing in accordance with article 74 of the CACM Regulation.

Baltic CGM - Common grid model consisting of Baltic TSOs’ individual grid models and grid model data from adjacent third countries’ TSOs operating in the same synchronous area.

Identified Constraint - is a couple of elements composed by one (or more) assessed elements and the contingency leading to a violation of an operational security limit or a function of this operational security limit.

Assessed Element - is a network element for which the electrical state is evaluated in the regional or cross-regional process and which value is expected to fulfil regional rules function of the operational security limits. Assessed Elements list shall consist of Secured Elements and Scanned Elements.

Secured Element - is an Assessed Element on which operational security limit violations shall be identified and relieved in a coordinated way.

Scanned Element - is an Assessed Element on which operational security limit violations shall be monitored.

Coordinated operational security analysis (COSA) - means an operational security analysis performed by each TSO on a common grid model, in accordance with Article 72(2) - 72(4) of the SO Regulation.

Coordinated regional operational security assessment (CROSA) - means an operational security analysis performed by RSC on a common grid model, in accordance with Article 78 of the SO Regulation.

Quantitative approach – a mathematical computation method for determining a cross-border relevance of remedial action, defined in accordance with articles 15(4) and 15(5) of CSAM.

Qualitative approach - an empirically based method for determining a cross-border relevance of remedial action.

Abbreviations

CGM – common grid model;

IGM – individual grid model;

ROSC – regional operational security coordination;

RA – remedial action;

XRA – cross-border relevant remedial action;

RSC – regional security coordinator;

NRA – national regulatory authority;

RT – reference time;

DA – day-ahead;

ID – intraday;

CNE – critical network element;

HVDC – high-voltage direct current;

XNE - cross-border relevant network element;

OPDE – operational planning data environment;

2. General provisions for regional operational security coordination process

1. All TSOs of Baltic CCR and Baltic RSC shall manage operational security limits violations and RAs that are deemed internal and cross-border relevant within Baltic CCR, in a coordinated way with the affected TSOs for day-ahead and intraday CROSA processes.
2. All TSOs of the Baltic CCR and Baltic RSC shall perform regional operational security coordination in day-ahead and intraday timeframes for Baltic CCR in accordance with the provisions of this document.
3. *Coordinated operational security analysis* (hereafter referred to as COSA) process shall be performed by each TSO for the DA and ID timeframe processes. COSA requires the TSO to perform contingency analysis on year-ahead, DA and ID CGMs to ensure that any contingency does not create situation where operational security limits are exceeded in its control area.
4. *Coordinated regional operational security assessment* (hereafter referred to as CROSA) shall be performed by Baltic RSC in coordination with TSOs for the DA and ID timeframe processes. CROSA requires the Baltic RSC to perform regional operational security assessment at least to all TSOs of the capacity calculation region. If a constraint is detected, it shall recommend to the relevant TSO the most effective and economically efficient remedial action (hereinafter – RA). Baltic RSC also coordinates the preparation of RAs with and among TSOs to enable coordinated activation of RAs in real-time by TSOs and cross-border relevant remedial actions (XRAs) with other RSCs.
5. Prior to the start of the ROSC process for IGM preparation purposes, each TSO shall have the right to perform a local preliminary assessment in order to detect any violations of operational security limits on internal grid elements. Each TSO may choose whether or not to relieve violations of operational security limits on internal network elements using non-cross-border relevant remedial actions.
6. When preparing IGMs, each TSO shall include any non-cross-border relevant remedial actions resulting from the local preliminary assessment.
7. Each Baltic TSO shall inform all TSOs of Baltic CCR and Baltic RSC about any RA inclusion in its IGM.
8. Baltic RSC shall perform CROSA on the basis of the CGM, the contingency list and the operational security limits provided by TSOs. It shall deliver the results of the CROSA at least to all TSOs of Baltic CCR. When it detects a constraint, it shall recommend to the relevant TSOs the most effective and economically efficient RAs and may also recommend RAs other than those provided by the TSOs.

9. All TSOs shall ensure that the principles of cost-sharing of XRAs determined in accordance with Baltic CRCCS Methodology are treated in a consistent way. In addition to this, the additional cost sharing principles are determined in Article 5.7 of these Common Provisions.

3. Definition of input data for coordinated operational security analysis processes

3.1 Contingency list

1. Each TSO of Baltic CCR shall establish the list of contingencies to be analysed in DA and ID security analysis processes in accordance with article 33 of the SO Regulation.
2. Each TSO of Baltic CCR shall provide contingency list to Baltic RSC which shall be used for DA and ID security analysis processes.
3. If necessary, each TSO of Baltic CCR shall update its contingency list and provide updated contingency list to Baltic RSC.
4. Baltic RSC shall create a common contingency list to be used during CROSA processes based on the latest individual list provided by each TSO of Baltic CCR for DA and ID security analysis processes.
5. Baltic RSC shall make consistency check of provided Contingency list in accordance to article 4.1.
6. In case if data is inconsistent and there is sufficient time until further CROSA process steps, Baltic RSC shall inform relevant TSO. TSO shall send corrected contingency list. In case if data is inconsistent and there is insufficient time until further CROSA process steps, Baltic RSC shall use the latest available contingency list.
7. Baltic RSC shall use the latest available common contingency list in DA and ID CROSA processes in Baltic CCR.

3.2 Assessed Elements, XNEs and operational security limits

1. Each TSO of Baltic CCR shall define the list of Assessed Elements which are relevant for CROSA in Baltic CCR, considering its observability area and operational security limits in accordance with article 25 of the SO Regulation. Each TSO shall not include any reliability margin to operational security limits. Assessed Elements list shall consist of Secured Elements and Scanned Elements.
2. Secured Elements shall be all critical network elements (hereafter referred to as CNEs) and all network elements which voltage level is equal or above 330 kV and all HVDC systems.
3. Each TSO of Baltic CCR, which is a part of more than one CCR, shall have the right to exclude any element from the Secured Elements list which is subject to CROSA within other CCR.
4. The cross-border relevant network elements of Baltic CCR (hereafter referred to as XNEs) are Secured Elements defined in accordance with paragraph 2 of this article.

5. Each TSO of Baltic CCR shall have the right to exclude any element from Secured Elements list of their own control area, except CNEs, if all TSOs of Baltic CCR agree.
6. Each TSO of Baltic CCR may define Scanned Elements which shall be part of CROSA process.
7. Scanned Elements can be any element with a voltage level lower than 330 kV which is modelled in the IGM and any element excluded from the Secured Elements list.
8. Each TSO of Baltic CCR shall provide Assessed Elements list to Baltic RSC which shall be used for DA and ID security analysis processes.
9. If necessary, each TSO of Baltic CCR shall update its Assessed Elements list and provide updated Assessed Elements list to Baltic RSC.
10. Baltic RSC shall create a common Assessed Elements list to be used during CROSA processes based on the latest individual list provided by each TSO of Baltic CCR and share the common list with TSOs of Baltic CCR.
11. Baltic RSC shall make consistency check of provided Assessed Elements list in accordance to article 4.1.
12. In case if data is inconsistent and there is sufficient time until further CROSA process steps, Baltic RSC shall inform relevant TSO. TSO shall send corrected Assessed Elements list. In case if data is inconsistent and there is insufficient time until further CROSA process steps, Baltic RSC shall use latest available Assessed Elements list.
13. Baltic RSC shall use the latest available Assessed Elements list in DA and ID CROSA processes in Baltic CCR.

3.3 Remedial actions

1. Each TSO of Baltic CCR shall design RAs in accordance with article 14 of CSAM.
2. When preparing RAs, each TSO of Baltic CCR shall consider RAs defined in accordance with article 22 of the SO Regulation.
3. All TSOs of Baltic CCR, in coordination with Baltic RSC, shall identify whether a RAs prepared in accordance with paragraph 1 of this Article are cross-border relevant using the rules described in Article 5.1.
4. Provided RA data shall at least contain this information:
    a. RA availability timeframe;
    b. Expected cost;
    c. Activation time;
    d. Any additional information which is relevant for RA application.
5. When preparing RAs, each TSO of Baltic CCR shall consider restrictions which may limit the usage of RAs. At least following types of restrictions shall be considered:
    a. Technical limitations such as ramping restrictions, min/max output power, min/max redispatch or power change through HVDC systems;
    b. Operational restrictions and usage rules such as switching limitations, available range of taps, dependencies between topology measures;
    c. Procedural restrictions resulting from timing issues due to local or regional processes.

6. Baltic CCR TSOs shall provide the information on possible restrictions identified in accordance with article 3.3.5(a)-(c) to the Baltic RSC together with the list of available RAs.

3.4 Individual and common grid model provisions

1. All TSOs of Baltic CCR shall prepare Individual Grid Model (hereafter referred to as IGM**)** which should be used in security analysis processes. IGMs shall be provided to the operational data planning environment (hereafter referred to as – OPDE) according to article 70(2) of the SO Regulation.
2. OPDE shall be used for IGM and CGM data exchange between TSOs and Baltic RSC.
3. All TSOs of Baltic CCR shall have the right to perform a local preliminary assessment and choose whether to relieve operational security limit violations in its IGM.
4. All TSOs of Baltic CCR may include in its IGM any non-cross-border relevant preventive RAs, obtained during local preliminary assessment.
5. All TSOs of Baltic CCR shall include in its IGM preventive RAs, which were agreed and coordinated during the previous CROSA processes.
6. Baltic TSOs of Baltic CCR shall inform Baltic RSC about any included RAs in their IGMs.
7. Baltic RSC shall have the right to download those IGMs which are necessary for Baltic CGM creation.
8. Baltic RSC shall merge IGMs of Baltic TSOs into Baltic CGM including relevant parts of grid models of same synchronous area if necessary.
9. IGMs and CGM (Baltic CGM) shall be prepared according to common grid model methodology developed in accordance with article 70(1) of the SO Regulation.

4. Provisions for regional security coordinator

4.1 Data consistency evaluation

1. Baltic RSC shall monitor consistency and correctness of input data provided by each TSO of Baltic CCR which is defined in article 3 of these Common Provisions considering at least:
    a. Files format correctness;
    b. Data consistency within IGM and CGM;
    c. Data consistency within previous CROSA processes and timeframes;
2. Baltic RSC shall check the consistency between included RAs in the IGM by each Baltic TSO and information shared in accordance with articles 2.7 and 3.4.5. In case of inconsistency Baltic RSC shall inform relevant TSO about this fact and obtain explanation from the TSO with corrected data.
3. If Baltic RSC identify issues or incorrect information in provided input data, then Baltic RSC shall inform relevant TSOs and request the data correction and updates.

4.2 CROSA within Baltic CCR

1. CROSA shall be performed for DA timeframe in accordance with article 6 and for ID timeframe in accordance with article 7.
2. Baltic RSC shall perform CROSA based on Baltic CGM created in accordance with article 3.4.
3. All TSOs of Baltic CCR shall exchange with relevant TSOs and Baltic RSC the information on available RAs for DA and ID CROSA processes which can be used in Baltic CCR.
4. Baltic RSC shall gather all the data needed to perform the CROSA, including:
    a. common list of contingencies, in accordance with article 3.1;
    b. common list of Assessed Elements, in accordance with article 3.2;
    c. list of available RAs in accordance with articles 3.3 and 5.3 with determined their cross-border relevance in accordance with Article 5.2.
5. Baltic RSC shall assess the completeness and consistency of each input data file provided by each TSO of Baltic CCR in accordance with article 4.1. In case of any inconsistency in the delivered files, the Baltic RSC shall report this fact to the relevant TSO and request their data correction and updating.
6. When performing CROSA, Baltic RSC shall:
    a. perform operational security analysis (which covers power flow and contingency analysis) and identify operational security violations for DA and ID planning processes in N-situation and in (N-1) situation;
    b. provide operational security analysis results to all TSOs of Baltic CCR;
    c. recommend to the relevant TSOs RAs which would relieve operational security violations on Secured elements identified during CROSA in accordance with article 5.4;
    d. coordinate the TSOs acceptance of proposed RAs and share the information about the agreed RAs between with all TSOs of Baltic CCR.
7. Baltic RSC shall perform the CROSA in accordance with article 30 of CSAM, taking into account the following conditions:
    a. Baltic RSC shall exchange the results of the CROSA process with relevant RSCs of adjacent CCRs for cross-regional coordination.
    b. Baltic RSC shall coordinate with RSCs of adjacent CCRs the operational security violations on the overlapping XNEs in accordance with article 27 of CSAM and its amendment.
8. Baltic RSC shall inform all affected TSOs about the results of such cross-regional coordination.

4.3 RAs monitoring

1. Baltic RSC during CROSA processes shall check the correct inclusion of the agreed RAs in TSOs IGMs for relevant timeframes.

2. If Baltic RSC identifies that previously agreed RA has not been included in the IGM by a TSO, Baltic RSC shall contact the relevant TSO. Informed TSO shall fix the issues and provide updated IGM for further CROSA process steps.

5. RAs preparation, coordination and activation provisions

5.1 Identification of XRAs

1. All TSOs of Baltic CCR shall qualitatively identify the cross-border relevance of each RA in accordance with articles 14 and 15 of CSAM. In case of a disagreement of the results, the TSOs and Baltic RSC shall apply a quantitative approach in accordance with article 15(4) and article 15(5) of CSAM.
2. In case of using quantitative approach, the assessment shall be done at least on the XNEC elements in accordance with article 15(4) of CSAM.
3. In case of using quantitative approach, all RAs shall be considered as cross-border relevant which influence factor for at least one element defined in accordance with paragraph 2 is greater than 5%.
4. TSOs of Baltic CCR may delegate the task of performing calculations of RA influence factors in case of quantitative approach to Baltic RSC.
5. All RAs that are not identified as cross-border relevant shall be deemed as non-cross-border relevant.

5.2 Exchanging the information of the available RAs inside CCR

1. All TSOs of Baltic CCR shall provide the list of available RAs to concerned TSOs and Baltic RSC for the purpose of DA and ID CROSA processes in Baltic CCR. The list of available RAs shall be updated depending on TSOs' needs. TSO shall inform other TSOs and Baltic RSC about any updates of this list.
2. When providing to Baltic RSC the list of RAs, each TSO shall also consider and provide already agreed RAs from previous coordinated regional operational security assessments of the same MTU, except if:
    a. an unforeseen event has made a RA unavailable, or
    b. the RA has become technically unavailable, or
    c. a new more effective and efficient RA has become available.
3. If RA from previous CROSA process is no longer available, TSO shall provide reason to Baltic RSC, why RA is not available for CROSA process.

5.3 Exchanging the information of the available RAs cross-CCR

1. Baltic RSC shall coordinate with RSCs of adjacent CCRs during the CROSA process, any usage of RA which has the impact across CCR(s) (hereafter referred to as cross-CCR overlapping XRA).
2. Baltic RSC shall exchange all relevant results of the CROSA process within Baltic CCR and with RSCs of adjacent CCRs in order to coordinate cross-CCR overlapping XRAs between Baltic CCR and adjacent CCRs.
3. TSOs in coordination with RSCs shall relieve congestions on overlapping XNEs and shall coordinate cross-CCR overlapping XRAs impacting these overlapping XNEs in

accordance with the proposal for amendment to be developed in accordance with article 27(3) of CSAM.

4. Baltic RSC shall inform all TSOs about the results of the coordination with RSCs of adjacent CCRs on respective cross-CCR overlapping XRAs.

5.4 Identification of the most effective and economically efficient RAs

1. In DA and ID CROSA processes, Baltic RSC shall make the recommendation for the implementation of the most effective and economically efficient RAs to the concerned TSOs.
2. If necessary, Baltic RSC shall assess in coordination with the concerned TSOs and RSCs of adjacent CCRs the effectiveness and economic efficiency of RA prior to the implementation in a DA and ID CROSA processes.
3. When the Baltic RSC recommends RAs, it shall primarily recommend non-costly RAs. If there are no non-costly RAs which relieve operational security limit violations or their efficiency is insufficient, then Baltic RSC shall recommend also costly RAs.

5.5 Coordination of RAs

1. TSOs and Baltic RSC shall relieve congestions on Secured Elements and shall coordinate XRAs impacting these Secured Elements in accordance with the proposal for amendment to be developed in accordance with article 27(3) of CSAM.
2. In case of a detected violation of operational security limits, Baltic RSC shall recommend to the concerned TSO an appropriate RA from the available RAs provided by the TSOs. Baltic RSC may also recommend RAs other than those provided by the TSOs. Such kind of recommendation for RA shall be justified by Baltic RSC and validated by the concerned TSO.
3. When recommending RA in accordance with paragraph 2 of this article, Baltic RSC shall take into account possible restrictions identified in accordance with article 3.3.6 which may limit its usage.
4. RAs identified for relieving operational security limit violations in accordance with paragraph 3 of this article:
    a. shall not lead to additional violations of operational security limits on Scanned Elements;
    b. should not worsen existing operational security limit violations on Scanned Elements.
5. Each TSO shall assess whether the recommended RAs meet the following conditions:
    a. the RA is considered available for the specific market time unit in a consistent manner from the time frame of its decision in the coordination process up to all the subsequent timeframes of security analyses including the real time;
    b. the RA should relieve violations on the Secured Elements;
    c. the RA is not setting the affected TSO’s grid in an alert or emergency state based on the CGM used in the coordination process;

   d. the RA is not leading to any violations of operational security limits on Assessed Elements after the simulation of the corresponding contingency based on the CGM used in the coordination process;
   e. the RA is considered the most effective and economically efficient RA to relieve the congestion.
6. When the concerned TSO accepts the proposed RA, this RA shall be deemed agreed and included in the IGM, updated by a TSO according to article 21 of CSAM.
7. When a TSO rejects the recommended RA, the TSO shall provide an explanation for this decision to the Baltic RSC and the other affected TSOs. The concerned TSO shall identify with the Baltic RSC and other TSOs alternative RAs to relieve the operational security limits violations or leave the violation if there is possibility to solve it during the next CROSA process.

5.6 Activation of RAs

1. Each TSO shall activate the RAs agreed in DA and ID CROSA processes in due time.
2. Where security violations remain unsolved at the end of each coordination process, the concerned TSOs shall agree on the necessary RAs in real-time operation in order to coordinate the management of these remaining violations of operational security limits.
3. If RAs agreed during DA and ID CROSA processes and activated in relevant timeframe turn out to be insufficient to solve all congestions in real time, affected TSO shall activate any other available RAs in real time operations in order to maintain operational security. Involved TSOs shall inform Baltic RSC about activated additional RAs.
4. The following conditions for the activation of the proposed RA shall be met:
   a. this RA is considered available in a consistent manner from the time frame of its decision to all the subsequent timeframes of security analyses, up to real time,
   b. this RA is considered the most effective and economically efficient to relieve violations of operational security limits,
   c. when this RA is preventive, it shall not set the affected TSO’s grid in an alert or emergency state based on the CGMs used for its decision,
   d. when this RA is curative, it is not leading to a violation of an operational security limit in the affected TSO’s grid after the simulation of the corresponding contingency based on the CGMs used for its decision.
5. If an agreed RA becomes unnecessary, the concerned TSO can decline an activation of a RA or can deactivate an already activated RA. The concerned TSO shall ensure that declining an activation respectively the deactivation of the RA is not deemed cross-border impacting and does not affect other TSOs. The concerned TSO shall provide an explanation for this decision to Baltic RSC and the other TSOs.

5.7 Sharing of the costs of RAs

1. The cost sharing principles for XRA agreed in the DA and ID CROSA processes and in real-time operations shall apply to the following situations:
    a. Cost sharing principles of XRAs implicated by CROSA processes on a XNE for which the costs attributed to them shall be shared among the involved TSOs according to “Baltic CCR TSOs common methodology for redispatching and countertrading cost sharing in accordance with article 74 of the Commission Regulation (EU) 2015/1222 of 24 July 2015 establishing a guideline on capacity allocation and congestion management“.
    b. In situations where XRAs are activated to relieve violations on XNE that belongs solely to one TSO control area (i.e. not cross-border interconnections), the costs attributed to XRAs shall be covered solely by the XNE connecting TSO.
    c. In situations where non-XRAs are activated, the costs of RAs shall be covered by TSO in that control area where the violations of the network elements were relieved.

6. Day-ahead CROSA

1. All TSOs of Baltic CCR in coordination with Baltic RSC shall perform DA CROSA managing violations of operational security limits and XRAs within Baltic CCR.
2. Baltic DA CROSA shall be performed in accordance with articles 23 and 33 of CSAM. The local aspects including data provision, coordination of results applied in Baltic region should be followed as described in Annex 1 (Table 1) of these Common Provisions.
3. CROSA in DA timeframe shall be performed on the basis of a best forecast approach which shall be established in accordance with the following:
    a. Each TSO shall not include any reliability margin to its operational security limits in accordance with article 3.2.1.
    b. IGMs and subsequent CGMs shall include load and intermittent generation forecasts, market results, schedules and planned topology of the transmission system in accordance with article 70(3) of the SO Regulation.
    c. RAs shall be included in the IGMs and the subsequent CGMs in accordance to article 3.4.5.
4. DA CROSA process steps shall be performed during T0 to T5 reference time (hereafter referred to as RT) according to Annex 1 (table 1) and article 33(1) of CSAM. The default values shall apply: T0=18.00 CET; T1= 19.00 CET; T2=20.00 CET; T3=20.45 CET; T4=21.30 CET; T5= 22.00 CET. If possible, to implement, all TSOs of Baltic CCR shall have the right amend timings between T0 to T5 during implementation phase according to Baltic CCR peculiarities if this does not conflict with cross-CCR coordination procedures and commonly agreed processes within other CCRs.
5. Where violations of operational security limits remain at the end of the DA CROSA, the concerned TSOs and Baltic RSC shall agree on the objectives and the needed

steps to follow in intraday, in order to improve the management of these remaining violations. The objectives could be such as but not limited to:

   a. Third countries influence
   b. Time restrictions in order to perform CROSA on time

6. Concerned TSOs of Baltic CCR and Baltic RSC shall organise a teleconference in order to validate outcomes of DA CROSA process.

7. Intraday CROSA

1. All TSOs of Baltic CCR in coordination with Baltic RSC shall perform ID CROSA and coordinate XRAs within Baltic CCR.
2. Baltic ID CROSA shall be performed in accordance with the process description introduced in Annex 1 (Table 2) of these Common Provisions, taking into account provisions introduced in article 24 of CSAM.
3. ID CROSA process shall be performed at least three times a day. The following reference timing for ID CROSA shall apply: 00:00, 08:00, and 16:00 CET, which will cover at least all market time units of following eight hours horizons from the reference time. Additional timeframes or extended horizons shall be agreed among TSOs upon their request and technical feasibilities during implementation or operational phases.
4. ID CROSA shall be performed on the basis of a best forecast approach, where the forecasted situation of each timestamp in the ID timeframe shall be established in accordance with Article 6.3(a)-(c).
5. When the results of the CROSA have significantly evolved with a regional impact compared to the previous ones, then the affected TSOs shall coordinate with the Baltic RSC, in order to:
   a. Share information about the significant changes of results, at least flows;
   b. Agree on change of previously agreed RA or on new XRA which may become required due to moving closer to or exceeding the operational security limits.
6. Baltic RSC shall ensure in ID CROSA that:
   a. violations of operational security limits on XNE with contingency identified are relieved using at least the RAs provided by TSOs. If violation is not relieved, then Baltic RSC shall strive to find and recommend additional available RA following the rules described in article 5.5.2.
   b. each TSO affected by XRA is informed about the violations of operational security limits to be solved by this RA.
7. When the conditions for implementation of RAs in accordance with article 5.5 are not met, each affected TSO shall accept or reject the implementation of the proposed RA. In case of rejection of the RA by one or several TSO(s) of Baltic CCR, the concerned TSO(s) shall provide an explanation for the decision.
8. All TSOs of Baltic CCR shall consider the results and agreed RAs of the ID CROSA in real-time operation. Where security violations remain unresolved at the end of each ID CROSA, the concerned TSOs shall activate necessary actions in real-time operation in accordance with article 5.6.3 and coordinate the management of these remaining violations of operational security limits.

8. Organisation of ROSC

8.1 Governance and operation of regional security coordinator

1. Baltic RSC shall be the service provider for the TSOs of Baltic CCR. Baltic RSC shall perform the tasks delegated by the TSOs of Baltic CCR in accordance with Article 9 of these Common Provisions.
2. Baltic RSC shall
    c. provide to all TSOs of Baltic CCR coordination services for the secure and efficient operation of the transmission system;
    d. build consistent regional data according to Article 3 of these Common Provisions;
    e. facilitate regional operational security coordination and perform the coordinated regional operational security assessment;
    f. make recommendations to TSOs of Baltic CCR in relation to the services they provide; and
    g. support the harmonisation of operational procedures and standards supporting TSOs of Baltic CCR to maintain security of supply.
3. Parties of the Baltic RSC Agreement shall be responsible for the operation of the Baltic RSC office(s) and each of these party shall take all necessary measures and allocate necessary and agreed resources enabling the office(s) to operate and deliver the agreed coordination services in accordance with Article 9.3.
4. The overall cooperation between the TSOs of Baltic CCR shall be governed by Baltic CCR steering committee.
5. The security of supply will remain the responsibility of each individual TSO of Baltic CCR according to national laws and regulations. The responsibility for secure system operation and any decision taken based on services provided by Baltic RSC shall remain with the TSOs of Baltic CCR.

8.2 Regional Security coordinator governing area

1. Baltic RSC governing area is equal to area defined according to the decision on Capacity Calculation Regions (CCRs) in accordance with article 15(1) of the Commission Regulation (EU) 2015/1222 for Baltic CCR and include following TSOs responsibility areas:
    a. Estonian TSO - “Elering AS”;
    b. Latvian TSO - “Augstsprieguma tikls”;
    c. Lithuanian TSO - “LITGRID AB”;
2. For coordinated regional operational security processes the following Baltic CCR’s cross-border interconnections are considered:
    a. Estonia - Finland, Estonian TSO and Finnish TSO;
    b. Estonia - Latvia, Estonian TSO and Latvian TSO;
    c. Latvia - Lithuania, Latvian TSO and Lithuanian TSO;
    d. Lithuania – Sweden, Lithuanian TSO and Swedish TSO;
    e. Lithuania – Poland, Lithuanian TSO and Polish TSO.

3. The responsibility for secure system operation and any decision taken based on services from Baltic RSC shall remain with the all TSOs of Baltic CCR.

9. Appointment of RSC and delegation of tasks to RSC

1. All TSOs of Baltic CCR appoint Baltic RSC as a *regional security coordinator* that will perform tasks listed in accordance with article 77(3) of the SO Regulation in the Baltic CCR.
2. Baltic RSC will perform the tasks listed in article 77 (3) of the SO Regulation in the Baltic CCR for all TSOs of Baltic CCR in a transparent and non-discriminatory manner.
3. In accordance with article 77(3) of the SO Regulation all TSOs of Baltic CCR delegate the following tasks to Baltic RSC, which should be carried out accordingly:
    a. regional operational security coordination in accordance with article 78 of the SO Regulation in order to support TSOs of Baltic CCR fulfil their obligations for the year-ahead, DA and ID timeframes in accordance with articles 34(3), 72 and 74 of the SO Regulation;
    b. building a common grid model in accordance with article 79 of the SO Regulation and article 3.4 of these Common Provisions.
    c. regional outage coordination in accordance with article 80 of the SO Regulation, in order to support TSOs of Baltic CCR to fulfil their obligations in accordance with articles 98 and 100 of SO Regulation;
    d. regional adequacy assessment in accordance with article 81 of the SO Regulation, in order to support TSOs of Baltic CCR fulfil their obligations in accordance with article 107 of SO Regulation.

9.1 Cooperation and coordination

1. Baltic RSC will implement the common provision of the tasks in close consultation and cooperation with All TSOs of Baltic CCR.
2. If Baltic RSC fails to provide service on a daily basis, all TSOs shall have the possibility to coordinate the process by and among themselves.
3. Until Baltic region is in the same synchronous area with continental Europe, the cooperation with adjacent RSCs operating in other regions (for example: Nordic RSC or TSCNET) should be handled through relevant TSOs of Baltic CCR. However, all TSOs of Baltic CCR have the right to delegate this task to Baltic RSC if the service could be fully implementable and provided by Baltic RSC.
4. CROSA process requires the interaction among the following TSOs:
    a. Estonian TSO - “Elering AS”;
    b. Latvian TSO - “AS Augstsprieguma tīkls”;
    c. Lithuanian TSO - “Litgrid AB”;
    d. Finnish TSO - “Fingrid Oyj”;
    e. Swedish TSO - “Affärsverket svenska kraftnät”;
    f. Polish TSO - “Polskie Sieci Elektroenergetyczne S.A.”.

5. The process requires the interactions with the following adjacent RSCs:

   a. Nordic RSC - RSC responsible for the CROSA processes in Nordic Capacity Calculation region.
   b. TSCNET, CORESO - RSCs responsible for the CROSA processes in Core Capacity Calculation region.
6. Any dispute between the RSCs and between Baltic RSC and all TSOs of Baltic CCR arising out of or in connection with this methodology shall be settled amicably between the TSOs of Baltic CCR. In case the dispute cannot be settled amicably between these parties within 60 calendar days after having been notified hereof, the dispute shall be finally settled by an arbitration process.
7. Baltic RSC with adjacent RSC(s) shall agree on a contractual framework defining the rules for operation of RSCs and the liability between RSCs.

10. Implementation timescale

1. All TSOs of Baltic CCR and Baltic RSC shall implement Common Provisions of Baltic ROSC without undue delay after all the following provisions are met:
   a. regulatory approval and implementation of the amendments of CSAM in accordance with article 27(3), article 21(6) and article 30 of CSAM;
   b. implementation of Common Grid Model Methodology in accordance with articles 67(1) and 70(1) of SO Regulation;
   c. development, testing and implementation of the IT tools, systems and procedures required to support the Common Provisions of Baltic ROSC;
2. The Common Provisions of Baltic ROSC shall be implemented taking into account the provisions set out in CRC and CRCCS Methodologies.
3. In accordance with article 46(5) of CSAM, all TSOs of Baltic CCR and Baltic RSC shall implement the requirements set forth in Common Provisions of Baltic ROSC concerning cross-regional operational security coordination in six months after the requirements have been implemented in accordance with paragraph 1 of this Article.
4. Until the CROSA processes will be developed and implemented in Baltic CCR and adjacent CCRs which will allow consistent and efficient coordination on TSOs level and on cross-regional level, the security analysis coordination shall be performed among TSOs of Baltic CCR
5. After the Baltic TSOs control areas synchronization with continental Europe, these Common provisions of Baltic ROSC shall be revised and amended as necessary.

11. Language

The reference language for the Common Provisions of Baltic ROSC shall be English. For the avoidance of doubt, where TSOs need to translate the Common Provisions of Baltic ROSC into their national language(s), in the event of inconsistencies between the English version and any version in another language, the relevant TSOs shall, in accordance with

national legislation, provide the relevant national regulatory authorities with an updated translation of the Common Provisions of Baltic ROSC.

Annex 1: Day-ahead and Intraday CROSA processes

Table 1. Day-ahead coordinated regional operational security assessment process

Step	From (Actor)	To	Time from (CET)	Time until (CET)	Activity for Actor	Output information
1	Relevant TSOs	[1]RSC(SA)		T0	Update: security limits for Assessed Elements; contingency list; RAs list;	Assessed element list, network elements security limits list, contingency list, RAs list
	Baltic TSOs	[2]RSC(CGM)			Perform local preliminary assessment, provide IGMs	IGMs
2	RSC (CGM)	RSC(SA), Baltic TSOs	T0	T1	Check the consistency of IGMs. If needed, request for corrected IGMs Creation of Baltic CGM	Request of correct IGMs Baltic CGM
3	RSC (SA)	TSOs	T1	T2	Perform a coordinated regional operational security assessment and share the results between relevant TSOs.	Report on detected constrains and propose RAs
4	TSOs	RSC(SA)	T2	T3	TSOs evaluate assessment results. TSOs shall: • inform RSCs about acceptance of RAs;	Coordinated RAs, updated IGMs

[1] RSC(SA) means RSC security analysis service
[2] RSC(CGM) means RSC individual and common grid model service

	Baltic TSOs	RSC(CGM)			Provide updated IGMs with agreed RAs	Updated IGMs with agreed RAs
5	RSC(CGM)	RSC(SA), Baltic TSOs			Creation of Baltic CGM RSCs provide updated CGM.	Updated Baltic CGM
6	RSC(SA)	TSOs	T3	T4	RSC perform a coordinated cross-regional operational security assessment	Report on detected constrains and propose RAs.
7	TSOs, RSC(SA)	TSOs-> RSC(SA) RSC(SA)-> TSOs	T4	T5	Final results coordination and consolidation session shall be according to Article 33 of SO Regulation. Final results should be agreed and confirmed between TSOs and RSCs.	Report on final results, agreed RAs and possible constraints.

Table 2. Intraday (ID) coordinated regional operational security assessment process

Step	From (Actor)	To	Time from (CET)	Time until (CET)	Activity for Actor	Output information
1	Relevant TSOs	RSC(SA)		[3]RT-95 ID	Update: security limits for Assessed Elements; contingency list; RAs list;	Assessed element list, network elements security limits list, contingency list, RAs list
2	Baltic TSOs	RSC(CGM)	RT-95 ID	RT-60 ID	Provide: IGMs with updated Net positions and flows	IGMs
3	RSC(CGM)	Baltic TSOs	RT-60 ID	RT-55 ID	Check the consistency of IGMs. If needed, request for corrected IGMs	Request of correct IGMs
4	RSC(CGM)	RSC(SA)	RT-55 ID	RT-45 ID	Creation of CGM	Provide CGM files for respective timeframes
5	RSC (SA)	TSOs	RT-45 ID	RT-20 ID	Perform SA. Provide assessment results to relevant TSOs.	Report on detected constrains and propose RAs
6	TSOs/ RSC(SA)	RSC(SA)/ TSOs	RT-20 ID	RT-10 ID	Report, distribute and coordinate the assessment results with TSOs of Baltic CCR and RSCs	Report on final results, agreed RAs and possible constraints.

[3] Note: For example, RT-95 means: 95 minutes until reference time