

ACER Decision on CSAM: Annex I

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

19 June 2019

Contents

| | |
|----------------------|---|
| Whereas | 5 |
| TITLE 1 | General Provisions |
| Article 1 | Subject matter and scope..... |
| Article 2 | Definitions and interpretation..... |
| TITLE 2 | Determination of influencing elements |
| Chapter 1 | Influence factor determination |
| Article 3 | Influence computation method |
| Article 4 | Possible relevance of dynamic aspects for influence assessment..... |
| Chapter 2 | Identification of influencing elements..... |
| Article 5 | Identification of observability area elements..... |
| Article 6 | Identification of external contingencies..... |
| TITLE 3 | Principles of coordination |
| Chapter 1 | Management of exceptional contingencies |
| Article 7 | Classification of contingencies |
| Article 8 | Occurrence increasing factors handling |
| Article 9 | Exceptional contingencies with a risk of high cross-control area impact..... |
| Article 10 | Establishment of the contingency list |
| Article 11 | Sharing of the contingency list..... |
| Chapter 2 | Evaluation of contingency consequences |
| Article 12 | Common agreement on cross-control area consequences..... |
| Article 13 | Assessment of consequences..... |
| Chapter 3 | Coordination of remedial actions |
| Article 14 | Designing of remedial actions |
| Article 15 | Identification of cross-border relevant network elements and remedial actions..... |
| Article 16 | Process for identifying cross-border relevant remedial actions |
| Article 17 | Principles for coordination of cross-border relevant remedial actions |
| Article 18 | Information on remedial actions availability and costs |
| Article 19 | Coordinated preventive remedial actions activation |
| Article 20 | Requirements for coordinated regional operational security assessments |
| Article 21 | Remedial actions inclusion in individual grid models..... |
| Chapter 4 | Realisation of operational security analyses with respect to uncertainty management and regional coordination..... |
| Article 22 | Long term studies (year-ahead up to week-ahead)..... |
| Article 23 | Day-ahead operational security analysis..... |

Methodology for coordinating operational security analysis

| | | |
|--|---|----|
| Article 24 | Intraday operational security analysis | 28 |
| Article 25 | Handling of extreme event..... | 29 |
| Chapter 5 | Cross-regional coordination..... | 30 |
| Article 26 | General requirements..... | 30 |
| Article 27 | Overlapping zones, XNEs and XRAs | 30 |
| Article 28 | Monitoring of inclusion of agreed remedial actions in the individual grid models | 32 |
| Article 29 | Back-up for the common grid model building task..... | 32 |
| Article 30 | Coordinated cross-regional operational security assessment..... | 32 |
| Article 31 | Investigation of possible additional remedial actions..... | 33 |
| Article 32 | Exchange of results..... | 33 |
| Article 33 | Regional and cross-regional day-ahead coordinated operational security assessment..... | 33 |
| Article 34 | Intraday coordinated regional operational security assessment..... | 35 |
| Article 35 | Outage planning coordination tasks | 35 |
| Article 36 | Regional adequacy assessment tasks | 35 |
| TITLE 4 | Forecast updates with respect to uncertainty management..... | 35 |
| Chapter 1 | Forecasts..... | 35 |
| Article 37 | Forecast of intermittent generation..... | 35 |
| Article 38 | Forecast of load..... | 36 |
| Chapter 2 | Grid model updates in intraday..... | 37 |
| Article 39 | Frequency of grid model updates | 37 |
| TITLE 5 | Governance and implementation..... | 37 |
| Chapter 1 | Governance | 37 |
| Article 40 | Identification and governance of common functions and tools..... | 37 |
| Article 41 | Coordination and information exchange with regional security coordinators ... | 38 |
| Article 42 | Data quality assessment | 39 |
| Article 43 | Monitoring of regional coordination | 39 |
| Article 44 | Towards probabilistic risk assessment..... | 40 |
| Chapter 2 | Implementation..... | 40 |
| Article 45 | Definition of common hours..... | 40 |
| Article 46 | Timescale for implementation..... | 41 |
| Article 47 | Language..... | 42 |
| Annex I | | 43 |
| AI.1 Influence threshold | | 43 |
| AI.2 Influence Computation Method..... | | 43 |

Methodology for coordinating operational security analysis

| | |
|---|----|
| AI.2.1 Power flow influence factor..... | 44 |
| AI.2.1.1 Network elements..... | 44 |
| AI.2.2 Voltage influence factor | 46 |

Whereas

- (1) This document describes a Methodology for coordinating operational security analysis (hereafter referred to as ‘CSAM’).
- (2) The CSAM takes into account the general principles and goals set in Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation (hereafter referred to as ‘SO Regulation’) as well as Commission Regulation (EU) 2015/1222 establishing a guideline on capacity allocation and congestion management (hereafter referred to as ‘CACM Regulation’), and Regulation (EC) No 714/2009 of the European Parliament and of the Council of 13 July 2009 on conditions for access to the network for cross-border exchanges in electricity (hereafter referred to as ‘Regulation (EC) No 714/2009’). The goal of the SO Regulation is to safeguard operational security, frequency quality and the efficient use of the interconnected system and resources. To facilitate these aims, it is necessary to enhance standardisation of operational security analysis at least per synchronous area. Standardisation shall be achieved through a common methodology for coordinating operational security analysis.
Article 75 of the SO Regulation constitutes the legal basis for the CSAM and defines several specific requirements that it should include at least: *(a) methods for assessing the influence of transmission system elements and significant grid users (‘SGUs’) located outside of a TSO’s control area in order to identify those elements included in the TSO’s observability area and the contingency influence thresholds above which contingencies of those elements constitute external contingencies; (b) principles for common risk assessment, covering at least, for the contingencies referred to in Article 33: (i) associated probability; (ii) transitory admissible overloads; and (iii) impact of contingencies; (c) principles for assessing and dealing with uncertainties of generation and load, taking into account a reliability margin in line with Article 22 of Regulation (EU) 2015/1222; (d) requirements on coordination and information exchange between regional security coordinators in relation to the tasks listed in Article 77(3); (e) role of ENTSO for Electricity in the governance of common tools, data quality rules improvement, monitoring of the methodology for coordinated operational security analysis and of the common provisions for regional operational security coordination in each capacity calculation region.*
- (3) With consideration of effective needs for standardisation, the CSAM also contains provisions: (i) to identify remedial actions which need to be coordinated between TSOs and to facilitate efficient remedial actions coordination at the regional level in accordance with the regional methodology to be developed later by all TSOs of a capacity calculation region pursuant to Article 76(1)(b) of the SO Regulation; (ii) to ensure efficient realisation of the operational security analyses for different timeframes under Articles 72 to 74 of the SO Regulation; and (iii) to ensure efficient and timely implementation of relevance assessment of outage coordination assets pursuant to the methodology under Article 84 of the SO Regulation and its necessary coordination with the common influence computation method under Article 75(1)(a) of the SO Regulation.
- (4) In accordance with Article 84(3) of the SO Regulation, the provisions of the CSAM, as regards the definition of the common influence computation method pursuant to Article 75(1)(a), are closely

Methodology for coordinating operational security analysis

- aligned with the common influence computation method provided in the methodology for assessing the relevance of assets for outage coordination in accordance with Article 84(1) of the SO Regulation.
- (5) The CSAM contributes to the objectives of the SO Regulation concerning the maintaining of the operational security throughout the Union by specifying provisions for all TSOs and RSCs on the coordination of system operation and operational planning, transparency and reliability of information on transmission system operation, and the efficient operation of the electricity transmission system in the Union.
 - (6) Furthermore, the CSAM ensures application of the principles of proportionality and non-discrimination; transparency; optimisation between the highest overall efficiency and lowest total costs for all parties involved; and use of market-based mechanisms as far as possible, to ensure network security and stability.
 - (7) In accordance with Recital (5) of the SO Regulation, synchronous areas do not stop at the Union's borders and can include the territory of third countries. The TSOs should aim for secure system operation inside all synchronous areas stretching on the Union. They should support third countries in applying similar rules to those contained in this Regulation. ENTSO for Electricity should facilitate cooperation between Union TSOs and third country TSOs concerning secure system operation.
 - (8) In conclusion, the CSAM contributes to the general objectives of the SO Regulation to the benefit of all TSOs, the Agency for the Cooperation of Energy Regulators, regulatory authorities and market participants.

TITLE 1 **General Provisions**

Article 1 **Subject matter and scope**

1. This Methodology establishes a coordinated operational security analysis in accordance with Article 75 of the SO Regulation.
2. This methodology shall cover the coordination of operational security analysis at Pan-European level and it applies to all TSOs, RSCs, DSOs, CDSOs and SGUs as defined in Article 2 of the SO Regulation.
3. TSOs from jurisdictions outside the area referred to in Article 2(2) of the SO Regulation may participate in the coordination of operational security analysis on a voluntary basis, provided that:
 - (a) for them to do so is technically feasible and compatible with the requirements of the SO Regulation;
 - (b) they agree that they shall have the same rights and responsibilities with respect to the coordination of operational security analysis as the TSOs referred to in paragraph 2;

Methodology for coordinating operational security analysis

- (c) they accept any other conditions related to the voluntary nature of their participation in the coordination of operational security analysis that the TSOs referred to in paragraph 2 may set;
 - (d) the TSOs referred to in paragraph 2 have concluded an agreement governing the terms of the voluntary participation with the TSOs referred to in this paragraph;
 - (e) once TSOs participating in the coordination of operational security analysis on a voluntary basis have demonstrated objective compliance with the requirements set out in (a), (b), (c), and (d), the TSOs referred to in paragraph 2, after checking that the criteria in (a), (b), (c), and (d) are met, have approved an application from the TSO wishing to participate on a voluntary basis in accordance with the procedure set out in Article 5(3) of the SO Regulation.
4. The TSOs referred to in paragraph 2 shall monitor that TSOs participating in coordination of operational security analysis on a voluntary basis pursuant to paragraph 3 respect their obligations. If a TSO participating in the coordination of operational security analysis pursuant to paragraph 3 does not respect its essential obligations in a way that significantly endangers the implementation and operation of the SO Regulation, the TSOs referred to in paragraph 2 shall terminate that TSO's voluntary participation in the coordination of operational security analysis process in accordance with the procedure set out in Article 5(3) of the SO Regulation.

Article 2

Definitions and interpretation

1. For the purposes of the CSAM, the terms used shall have the meaning of the definitions included in Article 3 of the SO Regulation, Article 2 of CACM Regulation and Article 2 of Commission Regulation (EU) No 543/2013 of 14 June 2013 on submission and publication of data in electricity markets. In addition, the following definitions shall apply:
 - (1) 'network element' means any component of a transmission system, including interconnectors, or of a distribution system, including a closed distribution system, such as a single line, a single circuit, a single HVDC system, a single transformer, a single phase-shifting transformer, or a voltage compensation installation;
 - (2) 'connecting TSO' means a TSO whose transmission system is connected directly or indirectly to a CDSO/DSO network;
 - (3) 'permanent occurrence increasing factor' means a factor that explains a permanent increase of the probability of occurrence of an exceptional contingency;
 - (4) 'temporary occurrence increasing factor' means a factor that explains a temporary increase of the probability of occurrence of an exceptional contingency;
 - (5) 'evolving contingency' means the loss of several network elements and/or grid users resulting from the occurrence of a contingency from the contingency list followed by the automatic or manual tripping of additional network elements which are in violation of their operational security limits;

Methodology for coordinating operational security analysis

- (6) ‘verifiable evolving contingency’ means an evolving contingency for which each and every step subsequent to the initial contingency can be simulated until a stable state is reached;
- (7) ‘design of remedial actions’ means the identification of resources available to be used as remedial actions;
- (8) ‘cross-border relevant network element’ or ‘XNE’ means a network element identified as cross-border relevant and on which operational security violations need to be managed in a coordinated way;
- (9) ‘cross-border relevant network element with contingency’ or ‘XNEC’ means an XNE associated with a contingency. For the purpose of this methodology, the term XNEC also cover the case where a XNE is used in operational security analysis without a specified contingency;
- (10) ‘XNE connecting TSO’ means the TSO responsible for the control area where the XNE is located or connected. In case of an interconnector, the TSOs on both sides of the interconnector shall be considered as XNE connecting TSOs;
- (11) ‘remedial action influence factor’ means a flow deviation on a XNEC resulting from the application of a remedial action, normalised by the permanent admissible loading on the associated XNE;
- (12) ‘cross-border relevant remedial action’ or ‘XRA’ means a remedial action identified as cross-border relevant and needs to be applied in a coordinated way;
- (13) ‘restoring remedial action’ means a remedial action that is activated subsequent to the occurrence of an alert state for returning the transmission system into normal state again;
- (14) ‘XRA connecting TSO’ means the TSO responsible for the control area where the XRA is located or connected. In case of an interconnector, the TSO executing the topological change shall be considered as XRA connecting TSO;
- (15) ‘XRA affected TSO’ means the TSO which is significantly impacted by the activation of the XRA;
- (16) ‘coordinated regional operational security assessment’ means an operational security analysis performed by a RSC on a common grid model, in accordance with Article 78 of the SO Regulation;
- (17) ‘coordinated operational security analysis’ means an operational security analysis performed by a TSO on a common grid model, in accordance with Article 72(3) and 72(4) of the SO Regulation;
- (18) ‘preventive remedial action’ means a remedial action that is the result of an operational planning process and needs to be activated prior to the investigated timeframe for compliance with the (N-1) criterion;

Methodology for coordinating operational security analysis

- (19) ‘agreed remedial action’ means a cross-border relevant remedial action for which TSOs in a region agreed to implement or any other remedial action for which TSOs have agreed that it does not need to be coordinated;
 - (20) ‘local preliminary assessment’ means an operational security analysis performed by a TSO to prepare an individual grid model;
 - (21) ‘delegating TSO’ means a TSO which has delegated tasks to a RSC in accordance with Article 77(3) of the SO Regulation;
 - (22) ‘overlapping XNE’ means an XNE on which the physical flows are significantly impacted by electricity exchanges in two or more CCRs or by XRAs from two or more CCRs;
 - (23) ‘overlapping XRA’ means an XRA that is able to address operational security violations on overlapping XNE;
 - (24) ‘curative remedial action’ means a remedial action that is the result of an operational planning process and is activated straight subsequent to the occurrence of the respective contingency for compliance with the (N-1) criterion, taking into account transitory admissible overloads and their accepted duration;
 - (25) ‘reference load’ means the average load defined as total consumption energy in the control area divided by the number of hours composing the year.
2. Where this Methodology refers to network elements, it includes HVDC systems.
 3. ‘IGM’ and ‘CGM’ respectively stand for ‘individual grid model’ and ‘common grid model’. ‘ENTSO- E’ stands for ‘ENTSO for electricity’. ‘RSC’ stands for ‘regional security coordinator’.

TITLE 2

Determination of influencing elements

Chapter 1

Influence factor determination

Article 3

Influence computation method

1. The influence computation method has the following characteristics:
 - (a) it is able to characterise the influence of the absence of one network element connected to a TSO or DSO/CDSO network on the power flow or voltage of another transmission network element;
 - (b) it is applicable on a year-ahead common grid model developed in accordance with Article 67 of the SO Regulation. This model may be complemented, as appropriate, by the TSO to represent the DSO/CDSO systems;

Methodology for coordinating operational security analysis

- (c) the influence is characterised with respect to the relative or absolute value of power flow or voltage variation and the result is able to be compared against thresholds.
2. Each TSO shall apply the influence computation method provided in Annex I for computing power flow influence factors, of transmission-connected network elements connected outside the TSO's control area, on network elements of its control area.
 3. Each TSO shall apply the influence computation method provided in Annex I for computing power flow influence factors, of network elements connected to transmission-connected DSO/CDSO networks located outside its control area, on network elements of its control area, provided that they are modelled in the CGMs used for the computation.
 4. Where the power flow influence factors do not sufficiently capture the network elements that can cause significant voltage variations in TSO's control area, this TSO shall have the right to use voltage influence factors in the determination of its observability area and external contingency list.
 5. Where applicable according to paragraph 4, each TSO shall inform affected TSOs about the decision to compute voltage influence factors and shall apply the influence computation method provided in Annex I for computing these factors of transmission-connected network elements connected outside its control area.
 6. Where applicable according to paragraph 4 each TSO shall apply the influence computation method provided in Annex I for computing voltage influence factors of network elements connected to transmission-connected DSO/CDSO networks located outside its control area. This TSO shall inform TSOs to which transmission-connected DSO/CDSO networks are connected to and are affected by application of this paragraph about its decision to compute voltage influence factors. In turn, each connecting TSO, shall inform of this application the affected transmission-connected DSO/CDSOs.
 7. Each connecting TSO shall inform the concerned DSOs/CDSOs located in its control area about any decisions to compute power flow and/or voltage influence factors of network elements of their systems. In addition, each connecting TSO shall be entitled to ask these DSOs/CDSOs for technical parameters and data with a reasonable limited depth proportional to the influence computation needs, in order to allow the inclusion of at least part of their networks in the TSO's individual grid models.
 8. When requested according to paragraph 7, each DSO/CDSO shall provide a single coherent set of data within three months after receiving the request, to enable the connecting TSO to incorporate the required part of DSO/CDSO networks in TSO's individual grid models established pursuant to paragraph 10 and 11.
 9. Each TSO shall use the common grid models established according to Article 67 of the SO Regulation, and complemented as needed pursuant to paragraph 11, when computing power flow and/or voltage influence factors of network elements connected directly or through a DSO/CDSO to another TSO's control area of the SO Regulation.
 10. When computing the influence of network elements constituting the grid of DSOs/CDSOs located in its control area, each TSO shall use the common grid models established according to Article 67 of the SO Regulation and complemented as needed pursuant to paragraph 7 to include additional network elements

Methodology for coordinating operational security analysis

than those required by the application of the methodology developed according to Article 67 of the SO Regulation.

11. Each TSO shall include in its individual grid model the relevant transmission-connected DSO/CDSO data model which it identifies as necessary for the computation of influence factors by another TSO.

Article 4

Possible relevance of dynamic aspects for influence assessment

1. Without prejudice to Article 38(1) of the SO Regulation, when a TSO needs to apply Article 38(6)(b) or Article 38(6)(c) of the SO Regulation to ensure a secure operation of its transmission system, this TSO shall have the right to request the support of concerned TSOs to use dynamic studies for assessing influence of the connectivity status or electrical values (such as voltages, power flows and rotor angles) of the network elements, power generating modules, and demand facilities connected outside its control area and connected to a transmission system. In that case, this TSO and the concerned TSOs shall define models, studies and criteria to be used for the assessment and inform their national regulatory authorities and relevant RSC(s) about their agreement. These models, studies and criteria shall be consistent with those developed in the application of Article 38 or 39 of SO Regulation.
2. When a TSO needs to apply Article 38(6)(b) or Article 38(6)(c) of SO Regulation to ensure a secure operation of its transmission system, this TSO shall have the right to use dynamic studies to assess influence of the connectivity or electrical values (such as voltages, power flows and rotor angles) of the network elements, power generating modules, and demand facilities located in transmission-connected DSOs/CDSOs networks located in its control area. In such a case, the TSO shall use models, studies and criteria, consistent with those developed in application of Article 38 or 39 of the SO Regulation.
3. Without prejudice to Article 38(1) of the SO Regulation, when a TSO needs to apply Article 38(6)(b) or Article 38(6)(c) of the SO Regulation to ensure a secure operation of its transmission system, this TSO shall have the right to request the support of concerned TSOs to use dynamic studies for assessing influence of the connectivity or electrical values (such as voltages, power flows and rotor angles) of the network elements, power generating modules, and demand facilities located in transmission-connected DSOs/CDSOs networks connected to other TSOs. In such a case, the TSO performing the computation will inform the TSOs which transmission-connected DSO/CDSOs are connected to about this decision and shall use models, studies and criteria consistent with those developed in application of Article 38 or 39 of the SO Regulation.
4. Each TSO, which transmission-connected DSO/CDSOs are connected to and are affected by the application of paragraphs 2 or 3, shall inform these transmission-connected DSO/CDSOs and concerned SGUs connected to these DSOs/CDSOs about the decision to use dynamic studies to assess their influence. In addition, each TSO shall be entitled to ask these DSOs/CDSOs and SGUs for the corresponding technical parameters and data, provided this request is proportional to the needs of the dynamic study.

Methodology for coordinating operational security analysis

5. When requested according to paragraph 4, each transmission-connected DSO/CDSO and each SGU shall provide a single coherent set of data within three months after receiving the request to enable the connecting TSO to incorporate the required part of their systems in models developed in application of Article 38 or 39 of the SO Regulation.
6. Each TSO, which transmission-connected DSO/CDSOs are connected to and are affected by the application of paragraph 2 or 3, shall share results of the performed assessment with these transmission-connected DSO/CDSOs and concerned SGUs.
7. Where one or more system elements are identified in application of paragraph 2, the concerned TSO shall inform its regulatory authority and relevant RSC(s) of the system elements identified with reasoning supporting this result.
8. Where one or more system elements are identified in application of paragraph 3, the TSO that performed dynamic studies and the TSOs which transmission-connected DSO/CDSO are connected to, shall inform their regulatory authorities and relevant RSC(s) of the system elements identified with the reasoning supporting this result.

Chapter 2

Identification of influencing elements

Article 5

Identification of observability area elements

1. Each TSO shall define its observability area in accordance with Article 3, Article 4 where applicable and the following paragraphs.
2. Each TSO shall aim at agreeing with each transmission-connected DSO/CDSO located in its control area, which network elements connected to this DSO/CDSO network will be part of its observability area based on qualitative assessment.
3. Where deemed necessary by the TSO, this TSO shall aim to agree with each non-transmission-connected DSO/CDSO located in its control area and its connecting DSO which network elements connected to this DSO/CDSO will be part of its observability area, based on a qualitative assessment.
4. If the TSO and the concerned DSO/CDSO do not agree, the identification of system elements will be done in accordance with Article 3 and where applicable Article 4.
5. Each TSO shall select threshold values inside the range of observability thresholds listed in Annex I that it shall use to determine its observability area in application of paragraphs 6 and 7. The threshold values shall be identical regardless of the network element whose influence is assessed by this TSO. Each TSO shall communicate to its RSC(s) and ENTSO-E those threshold values in time with the application of paragraph 1 and in accordance with Article 46(11). ENTSO-E shall collect those threshold values and shall publish them on its website at least once a year.

Methodology for coordinating operational security analysis

6. Each TSO shall include in its observability area:
 - (a) all transmission system elements of its control area;
 - (b) all network elements connected outside its control area which have an influence factor greater than the corresponding observability influence threshold values selected pursuant to paragraph 5;
 - (c) all network elements of transmission-connected DSOs/CDSOs located in its control area, identified in accordance with paragraph 2, or all network elements of transmission-connected DSOs/CDSOs identified in accordance with paragraph 4 that have an influence factor greater than the corresponding observability influence threshold values selected pursuant to paragraph 5;
 - (d) all network elements of non-transmission-connected DSOs/CDSOs located in its control area, identified in accordance with paragraph 3, or all network elements of non-transmission-connected DSOs/CDSOs identified in accordance with paragraph 4 that have an influence factor greater than the corresponding observability influence threshold values selected pursuant to paragraph 5;
 - (e) all network elements connecting this TSO's control area to another TSO's control area;
 - (f) additional network elements which are necessary to obtain a fully connected observability area;
 - (g) system elements identified in application of Article 4(1) to Article 4(3), where applicable;
 - (h) busbars to which the network elements previously identified in accordance with points ((a)) to (g) can be connected.
7. A TSO shall have the right to discard some network elements identified in accordance with points (b) to (d) of paragraph 6, provided their influence factor is not greater than the maximum value of the range of thresholds defined in Annex 1.
8. In case a TSO intends to include in its observability area network elements, power generating modules or demand facilities that are connected to the transmission system and not connected to a busbar, identified in accordance with paragraph 6, this TSO shall send a request to the concerned TSOs. The TSOs that receive the request are entitled to accept, propose an alternative solution or reject it, if operational security is not jeopardised.
9. TSOs shall have the right to agree to keep existing data exchange for system elements that are not identified in application of paragraph 6.
10. TSOs and DSOs shall have the right to agree to keep existing data exchange for elements that are not identified in application of paragraph 6.
11. Each TSO shall re-assess its observability area in accordance with paragraphs 2 to 8 at least once every 3 years.
12. Between two mandatory assessments in accordance with paragraph 11, any new system element commissioned inside a TSO's observability area shall be included in its observability area. If the owner

Methodology for coordinating operational security analysis

of the new system element disagrees with such a qualitative approach, TSOs shall use the influence computation method in accordance with Article 3 and, where applicable, Article 4 for establishing the relevance of this system element.

13. After any assessment of its observability area or after new elements have been added in accordance with paragraph 12, the TSO shall inform the relevant RSC(s) about the scope its observability area.

Article 6

Identification of external contingencies

1. Each TSO shall define its external contingency list in accordance with Article 3, Article 4, where applicable, and the following paragraphs.
2. Each TSO shall select threshold values inside the range of external contingency thresholds listed in Annex 1 that it shall use to determine its external contingency list in application of paragraph 1. The threshold values shall be identical regardless of the network element whose influence is assessed by this TSO. Each TSO shall communicate to ENTSO-E those threshold values in time with the application of paragraph 1 and in accordance with Article 46(11). ENTSO-E shall collect those threshold values and shall publish them on its website at least once a year.
3. Each TSO shall include in its external contingency list at least:
 - (a) all contingencies of any single network element connected outside its control area which have an influence factor greater than the corresponding external contingency threshold values selected pursuant to paragraph 2;
 - (b) all contingencies of network elements located in transmission-connected DSOs/CDSOs networks connected to this TSO, which are located in the TSO's observability area and commonly agreed between the TSO and the DSO/CDSO according to Article 5(2). In alternative all contingencies of network elements of these DSOs and CDSOs, which are located in the TSO's observability area, and which have an influence factor greater than the corresponding external contingency threshold values selected pursuant to paragraph 2.
4. Each TSO shall have the right to complement its external contingency list with any of the generating modules and demand facilities connected to a busbar identified in accordance with Article 5.
5. All new system elements commissioned inside a TSO's observability area shall either be assessed in accordance with Article 3 and, where applicable, Article 4, or shall be included without any assessment in its external contingency list.
6. Each TSO shall re-assess its external contingency list in accordance with paragraph 2 to 4 at least once every 5 years.
7. ENTSO-E shall assess any interoperability issues stemming from different threshold values selected by all TSOs in accordance with paragraph 2 and report on its findings and proposals in accordance with Article 17 of the SO Regulation.

TITLE 3
Principles of coordination

Chapter 1
Management of exceptional contingencies

Article 7
Classification of contingencies

1. When building its contingency list as required by Article 33 of the SO Regulation, each TSO shall classify for its own control area:
 - (a) the following contingencies as ordinary:
 - (i) loss of a single line / cable;
 - (ii) loss of a single transformer;
 - (iii) loss of a single phase-shifting transformer;
 - (iv) loss of a single voltage compensation device;
 - (v) loss of a single component of a HVDC system such as a line or a cable or a single HVDC converter unit;
 - (vi) loss of a single power generation unit;
 - (vii) loss of a single demand facility.
 - (b) the following contingencies as exceptional:
 - (i) loss of network elements having common fault mode, meaning that a single fault (such as a fault on a busbar, HVDC grounding system, circuit breaker, measurement transformer etc.) will lead to the loss of more than one network element;
 - (ii) loss of overhead lines built on same tower;
 - (iii) loss of underground cables built in same trench;
 - (iv) loss of grid users having common process mode, meaning that the total or partial sudden loss of one grid user will lead to the total or partial loss of the others (for example: Combined cycle units etc.);
 - (v) loss of network elements/users simultaneously disconnected as a result of the operation of a Special Protection Scheme;
 - (vi) loss of multiple generation units (including solar and wind farms) disconnected because of a voltage drop on the network or system frequency deviation.
 - (c) the following contingencies as out-of-range:

Methodology for coordinating operational security analysis

- (i) loss of two or more independent lines;
 - (ii) loss of two or more independent cables;
 - (iii) loss of two or more independent transformers or phase shifter transformers;
 - (iv) loss of two or more independent grid users (power generating unit or demand facility);
 - (v) loss of two or more independent voltage compensation devices;
 - (vi) loss of two or more independent busbars;
 - (vii) loss of two or more independent components of a HVDC system such as lines, cables or HVDC converter units.
2. For any other type of contingency resulting in the simultaneous loss of one or several grid users or network elements and not listed above, each TSO shall classify them in one of the three categories (ordinary, exceptional or out-of-range) according to the definitions provided for in Article 3 of the SO Regulation.

Article 8

Occurrence increasing factors handling

1. Each TSO shall determine for each exceptional contingency the relevance and criteria of application of the following occurrence increasing factors:
 - (a) permanent occurrence increasing factors:
 - (i) specific geographical location;
 - (ii) design conditions;
 - (b) temporary occurrence increasing factors:
 - (i) operational conditions;
 - (ii) weather or environmental conditions;
 - (iii) life time or generic malfunction affecting the risk of failure.
2. When determining the relevance and criteria of application of occurrence increasing factors listed in point (b) of paragraph 1, each TSO shall consider operational, weather or environmental conditions in relation with the specifications and the current state of the equipment.
3. When determining the relevance of application of occurrence increasing factors listed in paragraph 1, each TSO shall take into account where available the history of incidents that occurred on the concerned network elements.

Article 9

Exceptional contingencies with a risk of high cross-control area impact

1. Where a TSO expects that exceptional contingencies located in another TSO's control area may lead to consequences above the consequences within the TSO's control area which are considered as acceptable with respect to its national legislation as referred to in Article 4(2)(e) of the SO Regulation, or, if no national legislation exists, with respect to its internal rules, and this other TSO does not include these exceptional contingencies in its contingency list because it does not identify occurrence increasing factors in accordance with Article 8, these TSOs may jointly establish an agreement on additional exceptional contingencies located in one of their control areas which shall be included in their contingency lists in order to ensure that the consequences in their control areas remain acceptable.
2. When establishing this agreement, these TSOs shall determine the maximum cost of remedial actions above which, the cost of fulfilment of operational security limits shall not be deemed proportionate to the risk. These TSOs shall take into account their national legislation as referred to in Article 4(2)(e) of the SO Regulation, or, if no national legislation exists, take into account their internal rules.
3. When establishing this agreement, these TSOs shall ensure that all affected TSOs are participating in the agreement.

Article 10

Establishment of the contingency list

1. When applying Article 33(1) of the SO Regulation, each TSO shall include in its contingency list at least:
 - (a) the ordinary contingencies;
 - (b) the exceptional contingencies fulfilling the application criteria of at least one of the permanent occurrence increasing factors;
 - (c) the exceptional contingencies fulfilling the application criteria of at least one of the temporary occurrence increasing factors when conditions are met;
 - (d) the exceptional contingencies which lead to consequences above the consequences within the TSO's control area which are considered as acceptable with respect to its national legislation as referred to in Article 4(2)(e) of the SO Regulation, or, if no national legislation exists, with respect to its internal rules.
2. In addition, each TSO part of an agreement established in accordance with Article 9 shall include in its contingency list where needed the identified exceptional contingencies.
3. In addition, each TSO shall include in its contingency list the external exceptional contingencies potentially endangering operational security of its transmission system in accordance with paragraphs 3 and 4 of Article 11.
4. When assessing the contingencies referred to in point (a) of paragraph 1, each TSO shall have the right to exclude those which will never lead to consequences above the consequences which are considered as

Methodology for coordinating operational security analysis

acceptable with respect to its national legislation or, if no national legislation exists, with respect to its internal rules.

5. When assessing the contingencies referred to in point (d) of paragraph 1, each TSO shall take into consideration whether the cost of remedial actions needed to maintain the consequences acceptable is deemed proportional to the risk with respect to its national legislation or, if no national legislation exists, with respect to its internal rules.

Article 11

Sharing of the contingency list

1. Each TSO shall inform without undue delay the TSOs whose observability area contains network elements of its contingency list and the relevant RSC(s) about any update of the exceptional contingencies fulfilling the application criteria of at least one of the permanent occurrence increasing factors.
2. Each TSO shall inform without undue delay the TSOs whose observability area contains network elements of its contingency list, and the relevant RSC(s), about any update of the exceptional contingencies that have the potential to fulfil the application criteria of at least one of the temporary occurrence increasing factors or when conditions are met that fulfil the application criteria of at least one of the temporary occurrence increasing factors.
3. When informed by another TSO pursuant to paragraph 1 or 2, each TSO shall assess whether this contingency endangers the operational security of its transmission system.
4. Each TSO shall inform without undue delay, when conditions are no longer met, the TSOs whose observability area contains network elements of its contingency list and the relevant RSC(s) about any update of the exceptional contingencies no longer fulfilling the application criteria of any temporary occurrence increasing factors.
5. Each TSO shall inform the relevant RSC(s) about the contingencies of their contingency list for which the TSO shall not be required to comply with the (N-1) criterion either:
 - (a) because the TSO decides not to comply with the (N-1) criterion in application of Article 35(5) of the SO Regulation; or
 - (b) because they are part of a set of contingencies jointly agreed in application of Article 12.
6. Each TSO shall inform the relevant RSC(s) about the contingencies identified in application of Article 9 in accordance with Article 78(1)(a) of the SO Regulation.

Chapter 2

Evaluation of contingency consequences

Article 12

Common agreement on cross-control area consequences

1. TSOs shall have the right to agree jointly in a multi-lateral agreement that a set of contingencies of their contingency lists do not respect the (N-1) criterion. The precondition for such a multi-lateral agreement is that the contingencies not respecting the (N-1) criterion have consequences limited to the contracting TSOs' control areas and considered as acceptable within each contracting TSO's control area with respect to their national legislation as referred to in Article 4(2)(e) of the SO Regulation or, if no national legislation exists, with respect to their internal rules. These TSOs shall inform all TSOs and RSCs about this agreement.
2. For each multi-lateral agreement pursuant to paragraph 1, the concerned RSC shall analyse the set of contingencies not respecting the (N-1) criterion for consequences on control areas of TSOs in the concerned capacity calculation region ('CCR') not taking part in the relevant multi-lateral agreement and report to its TSOs. The results of the analysis shall be shared with the affected TSOs and relevant RSCs.

Article 13

Assessment of consequences

1. In addition to Article 35(1) of the SO Regulation, each TSO shall assess the consequences of any contingency of its contingency list:
 - (a) by evaluating that the power deviation between generation and demand resulting of the occurrence of a contingency or from a verifiable evolving contingency does not exceed the reference incident, and that one of the following conditions is fulfilled:
 - (i) the operational security limits determined in accordance with Article 25 of the SO Regulation are respected on all network elements connected in its control area in compliance with Article 35(1) of the SO Regulation and there is no risk of propagating a disturbance to the interconnected transmission system; or
 - (ii) the occurrence of the contingency leads to a verifiable evolving contingency with consequences limited to the perimeter of the TSO's control area and considered as acceptable with respect to its national legislation as referred to in Article 4(2)(e) of the SO Regulation or, if no national legislation exists, with respect to its internal rules, in compliance with Article 35(5) of the SO Regulation;
 - (b) or by evaluating, with the support of the relevant RSC(s), that the power deviation between generation and demand resulting from the occurrence of a verifiable evolving contingency does not exceed the reference incident. In addition to that the occurrence of the contingency leads to consequences limited to the control areas of TSOs which are party to an agreement defined in

Methodology for coordinating operational security analysis

accordance with Article 12 and considered as acceptable within each TSO's control area with respect to its national legislation as referred to in Article 4(2)(e) of the SO Regulation or, if no national legislation exists, with respect to its internal rules provided there is no risk of propagating a disturbance to the rest of the interconnected transmission system.

Chapter 3 **Coordination of remedial actions**

Article 14 **Designing of remedial actions**

1. When TSOs and RSCs design remedial actions, they shall identify all the resources categorised in Article 22 of the SO Regulation that can be used as remedial actions, which are generally able to address operational security violations.
2. A remedial action can be designed as an individual action or as a combination of actions as defined in Article 22 of the SO Regulation.
3. A remedial action consisting of a combination of actions can be designed at least in the following cases:
 - (a) where the activation requires a specific combination; and
 - (b) where optimisation of remedial actions is unable to find that specific combination of remedial actions.
4. Where a remedial action consists of a combination of actions, its cross-border relevance shall be assessed for the effect of the combination.
5. When designing the remedial action consisting of a combination of actions, TSOs and RSCs shall not unduly restrict the capability of optimisation of remedial actions to identify the most effective and economically efficient remedial actions.
6. All remedial actions designed by TSOs and RSCs of a CCR shall be subject to the identification process for their cross-border relevance pursuant to Article 15.

Article 15 **Identification of cross-border relevant network elements and remedial actions**

1. The 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.
2. The common provisions for regional operational security coordination pursuant to Article 76(1) of the SO Regulation shall define the rules and/or criteria to establish the XNEs for which the costs attributed to them shall be shared among the involved TSOs and the XNEs for which the costs attributed to them

Methodology for coordinating operational security analysis

- shall be covered solely by the XNE connecting TSO(s), taking into account rules for cost sharing in accordance with Article 74 of the CACM Regulation.
3. In order to identify whether a remedial action designed in accordance with Article 14 is cross-border relevant, TSOs and RSCs shall use a quantitative or qualitative approach.
 4. In case of 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.
 5. In case of quantitative approach, at least those remedial actions for which the remedial action influence factors for at least one XNEC is higher than a threshold, defining a significant cross-border impact shall be considered as cross-border relevant. This threshold shall be equal to 5% unless a different threshold is justified and defined in the methodology for the preparation of remedial actions managed in a coordinated way established within the common provisions for regional operational security coordination pursuant to Article 76(1) of the SO Regulation.
 6. In case of qualitative approach, TSOs, in coordination with RSCs, shall qualitatively assess and agree on the cross-border relevance of remedial actions. In case of disagreement, the TSOs shall apply the quantitative assessment in accordance with paragraphs 4 and 5.
 7. In case of qualitative and quantitative approach, TSOs, in coordination with RSCs, shall define for remedial actions that can be applied in different quantities, such as redispatching, countertrading, change of set point on HVDC systems or change of taps on phase-shifting transformers, the quantity above which these remedial actions become cross-border relevant.
 8. In case of qualitative and quantitative approach, TSOs, in coordination with RSCs, shall define for each remedial action, the XRA connecting TSO(s) and XRA affected TSOs. In case of quantitative approach, the XRA affected TSOs shall be those TSOs having at least one affected XNEC for which the remedial action influence is higher than the threshold referred to in paragraph 5.

Article 16

Process for identifying cross-border relevant remedial actions

1. When preparing the methodology for the preparation of remedial actions managed in a coordinated way established within the common provisions for regional operational security coordination pursuant to Article 76(1) of the SO Regulation, all TSOs of each CCR shall jointly determine:
 - (a) rules on a process for establishing a common list of XRAs and the XRA affected TSOs, based on the identification pursuant to Article 15;
 - (b) rules on a process for establishing a list of remedial actions that are not cross-border relevant;
 - (c) the frequency of update of the previous items.

Methodology for coordinating operational security analysis

2. In day-ahead or intraday operational planning, when preparing a remedial action, each TSO and RSC shall assess the cross-border relevance of remedial actions that have not been assessed in application of paragraph 1.
3. During real time operation, if the system is in alert state, when preparing restoring remedial actions, each TSO shall assess the cross-border relevance of remedial actions that have not been assessed in application of paragraph 1.
4. During real time operation, if the system is in emergency state and only when operational conditions allow it, when preparing restoring remedial actions each TSO shall assess the cross-border relevance of remedial actions that have not been assessed in application of paragraph 1.

Article 17

Principles for coordination of cross-border relevant remedial actions

1. In day-ahead or intraday operational planning, all TSOs, in coordination with the RSC(s) of a CCR, shall manage in a coordinated way operational security violations on all cross-border relevant network elements with contingency considering all cross-border relevant remedial actions and taking into account the potential technical restrictions limiting the use of certain remedial actions. To this end, the RSC(s) shall make recommendations for the implementation of the most effective and economically efficient cross-border relevant remedial actions to the concerned TSOs. These TSOs shall implement such remedial actions in accordance with Article 78(4) of the SO Regulation and other relevant Union legislation, following the methodology for the preparation of remedial actions managed in a coordinated way developed in compliance with Article 76 of the SO Regulation.
2. When the TSOs identify that the activation of a specific XRA could lead to violations of voltage limits or dynamic limits, the TSO(s) facing such limits and the XRA connecting TSO(s) shall coordinate with the RSC(s) to define limitations on the activation of such XRAs. These limitations shall then be considered by the RSC(s) in coordination and optimisation of XRAs.
3. During real time operation, if the system is in alert state, when deciding on restoring remedial actions that have been identified as cross-border relevant in accordance with Article 16(3), each TSO shall manage them in a coordinated way with the affected TSOs. This shall be done by ensuring at least that every affected TSO is informed about the operational security limit violation(s) to be relieved by those remedial actions and has accepted the activation of those remedial actions. The concerned TSO shall inform, without undue delay, the relevant RSC(s) of the activation of such remedial actions.
4. During real time operation, if the system is in emergency state and only when operational conditions allow it, when deciding on restoring remedial actions that have been identified as cross-border relevant in accordance with Article 16(4), each TSO shall manage them in a coordinated way with the affected TSOs. This shall be done by ensuring at least that every affected TSO is informed about the operational security limit violation(s) to be relieved by those remedial actions and has accepted the activation of those remedial actions. The concerned TSO shall inform, without undue delay, the relevant RSC(s) of the activation of such remedial actions.

Methodology for coordinating operational security analysis

5. When the RSC recommends the activation of XRAs in accordance with paragraph 1, the XRA connecting TSO(s) shall, in accordance with Article 78(4) of the SO Regulation and other relevant Union legislation, plan and activate the recommended remedial action provided that:
 - (a) it is expected to be available in the real time;
 - (b) and it is not leading to violation of operational security limits, taking into account the violations from not activating the XRAs.
6. When the RSC recommends the activation of XRAs in accordance with paragraph 1 or when a TSO proposes a restoring XRA in accordance with paragraphs 3 and 4, the XRA affected TSO(s) shall, in accordance with Article 78(4) of the SO Regulation and other relevant Union legislation, agree on the recommended remedial action provided that it is not leading to violation of operational security limits, taking into account the violations from not activating the XRAs.
7. In case the XRA connecting TSO or the XRA affected TSO refuses the RSC's recommendation or TSO proposal in accordance with paragraph 5 and 6, the concerned TSO(s) shall, in accordance with relevant Union legislation, coordinate with the RSC(s) and other TSOs to identify, plan and activate alternative remedial actions.

Article 18

Information on remedial actions availability and costs

1. When designing remedial actions in application of Article 14 and Article 20 of the SO Regulation or when providing to the relevant RSCs the updated list of possible remedial actions in application of Article 78(1)(b) of the SO Regulation, each TSO shall verify availability and endeavour to ensure that the remedial actions which were available for the coordinated operational security analyses, coordinated regional operational security assessments or capacity calculations previously performed for the same timestamps remain available in the concerned operational planning time-frame in accordance with Article 72(1) of the SO Regulation.
2. Each TSO shall provide to the RSCs the best forecast on possible XRAs available for coordination.
3. Each TSO shall provide to the RSCs prior to coordination the information about the prices or costs of costly XRAs needed to identify the most effective and economically efficient XRAs. To this end, the XRAs resources shall provide in due time to the relevant TSOs all information necessary for calculating the prices and costs at which the activated XRA shall be settled or, in case these cannot be established, the expected or forecasted prices and costs.
4. When relieving a violation of operational security limits during a coordinated operational security analysis in application of Article 72 of the SO Regulation for day-ahead and intraday timeframes, and in line with the common provisions for regional operational security coordination developed pursuant to Article 76 of the SO Regulation, each TSO shall take into consideration all the remedial actions already agreed during capacity calculations, coordinated operational security analyses or coordinated regional

Methodology for coordinating operational security analysis

security assessments previously performed for the same timestamps, except the remedial actions which have become unavailable for technical reasons.

5. When a TSO wants to modify a remedial action, which has previously been managed in a coordinated way and agreed, this TSO shall again assess the cross-border relevance of the modified remedial action and where necessary manage it in a coordinated way with the affected TSOs in accordance with Article 17.

Article 19

Coordinated preventive remedial actions activation

1. Each TSO shall activate XRAs, assessed in accordance with Article 16, as preventive remedial actions at the latest time compatible with their activation lead-time if their need is confirmed by the latest coordinated operational security analysis or coordinated regional operational security assessment performed for the concerned timeframe.
2. When preparing the activation of the cross-border relevant remedial actions, managed in accordance with Article 17, as preventive remedial actions, in order to provide enough flexibility in the daily operational activities, each TSO shall have the right to decide to activate them earlier than when it is necessary with consideration of the operational conditions and provided that it does not introduce any operational security limit violations.

Article 20

Requirements for coordinated regional operational security assessments

1. Within the proposal for common provisions for regional operational security coordination in accordance with Article 76(1) of the SO Regulation, all TSOs of each CCR shall, in accordance with Article 21(1) of the SO Regulation, jointly define the rules on the process for determining the cross-border relevant network elements on which the operational security violations shall be managed in a coordinated way (i.e. cross-border relevant network elements), taking into account provisions of Article 15(1).
2. The common provisions for regional operational security coordination developed in accordance with Article 76(1) of the SO Regulation by all TSOs of each CCR shall ensure that, when coordinated regional operational security assessments are performed in application of Article 78 of the SO Regulation, the following objectives are met:
 - (a) agreed remedial actions are included in the individual grid models;
 - (b) all violations of operational security limits on the network elements identified in application of paragraph 1 are relieved using at least cross-border relevant remedial actions;
 - (c) every XRA affected TSO is informed about the operational security limit violations to be solved by this remedial action and has agreed to it; and
 - (d) the coordination of cross-border relevant remedial actions pursuant to this methodology and pursuant to the coordinated redispatching and countertrading methodology established in

Methodology for coordinating operational security analysis

accordance with Article 35 of the CACM Regulation is fully consistent and managed within a single coordination process.

Article 21

Remedial actions inclusion in individual grid models

1. When preparing individual grid models pursuant to Article 70 of the SO Regulation, each TSO shall include all remedial actions already agreed as a result of previous coordinated operational security analyses in accordance with Article 17(1) and Article 18(4) or previous coordinated regional operational security assessments in accordance with Article 78 of the SO Regulation.
2. When preparing individual grid models pursuant to Article 70 of the SO Regulation, each TSO shall have the right to perform a local preliminary assessment.
3. When performing a local preliminary assessment, and provided this is consistent with the common provisions developed as required by Article 76(1) of the SO Regulation, each TSO may choose whether or not to relieve operational security limit violations on:
 - (a) network elements identified in accordance with Article 20(1) if the TSO expects it to be relieved during the subsequent coordinated regional operational security assessment;
 - (b) any other network elements provided those operational security limit violations are likely to be solved by non-cross-border relevant remedial action;
 - (c) any other network elements provided those operational security limit violations are likely to be relieved by subsequent coordinated regional operational security assessment.
4. When preparing individual grid models pursuant to Article 70 of the SO Regulation, in addition to the remedial actions referred to in paragraph 1 and taking into account where applicable the results of the local preliminary assessment referred to in paragraph 2, each TSO may include any non-cross-border relevant remedial actions in accordance with Article 21(1)(a) of the SO Regulation.
5. Remedial actions included pursuant to paragraphs 1 and 4 shall be clearly distinguishable from the injections and withdrawals established in accordance with Article 40(4) of the SO Regulation and the network topology without remedial actions applied.
6. No later than eighteen months after the adoption of this methodology, all TSOs shall jointly develop a proposal for amendment of this methodology in accordance with Article 7(4) of the SO Regulation. The proposal shall complement this methodology with the rules on distinguishing between:
 - (a) up-to-date load and generation forecasts and network topology considered within the individual grid model which are not aiming at addressing expected operational security violations identified during the local preliminary assessment and are therefore not considered as remedial actions; and
 - (b) the expected generation and load, as well as, network topology considered within the individual grid model, which are aiming at addressing expected operational security violations identified during the local preliminary assessment and are therefore considered as remedial actions.

Chapter 4
Realisation of operational security analyses with respect to uncertainty management and regional coordination

Article 22
Long term studies (year-ahead up to week-ahead)

1. In order to improve the robustness of the analyses against uncertainties in the coordinated operational security analyses in accordance with Article 72(1)(a) or (b) of the SO Regulation and in the validation and amendment of year-ahead availability plans within outage coordination regions in accordance with Articles 98(3), 100(3) and 100(4) of the SO Regulation, when deemed necessary by the TSO, the TSO shall develop and apply local scenarios for its control area in addition to the scenarios required according to Article 65 of the SO Regulation.
2. In developing these additional scenarios, the TSO shall determine for which operational planning activities those additional scenarios are to be considered and shall inform the TSOs of its capacity calculation region or of its outage coordination region and the relevant RSC(s) about the content of those additional scenarios and their usage purpose.
3. Where a TSO identifies additional scenarios for coordinated operational security analysis in accordance with Article 72(1)(a) or (b) of the SO Regulation or for outage coordination in accordance with Articles 98(3), 100(3) and 100(4) of the SO Regulation, and these scenarios differ from the scenarios defined by all TSOs according to Article 65 of the SO Regulation, other TSOs shall assess the impact on their control area and, where so relevant, build their individual grid models for these additional scenarios.
4. Where a TSO defines additional scenarios for operational security analysis in accordance with Article 72(1)(a) or (b) of the SO Regulation, this TSO shall define, in coordination with other TSOs of the concerned capacity calculation region and the relevant RSC(s), which common grid models shall be used to study these additional scenarios. These additional common grid models shall be derived from the common grid models established pursuant to Article 67 of the SO Regulation, using appropriate substitutes or derived models where appropriate.
5. Where a TSO identifies additional scenarios for outage coordination in accordance with Articles 98(3), 100(3) and 100(4) of the SO Regulation, this TSO shall build, in coordination with other TSOs of the outage coordination region and the relevant RSC(s), grid models corresponding to these additional scenarios. These grid models shall be derived from the common grid models established pursuant to Article 67 of the SO Regulation, using appropriate substitutes or derived models where appropriate.
6. These additional common grid models shall be studied by relevant RSCs and TSOs by applying the methodology for coordinating operational security analysis in accordance with Article 76(1) of the SO Regulation and regional coordination operational procedure developed in accordance with 83(1) of the SO Regulation.
7. Each RSC shall check the presence of cross-regional impact in studying additional common grid models. In case of the existence of cross-regional impact, the RSC shall coordinate the building and analysis of

Methodology for coordinating operational security analysis

appropriate additional common grid models with relevant RSCs and respective TSOs while applying principles referred to in paragraphs 3 to 6.

8. Considering that reliability margins in line with Article 22 of the CACM Regulation and Article 11 of Commission Regulation (EU) 2016/1719¹ shall be taken into account for capacity calculation processes, and that the goal of the operational security analysis is to identify expected operational security limit violations and consequent remedial actions, each TSO shall not include any reliability margins to its operational security limits when evaluating the results of the operational planning activities.

Article 23

Day-ahead operational security analysis

1. Each TSO shall perform in day-ahead a coordinated operational security analysis on the basis of a best forecast approach where the forecasted situation of each timestamp of the next day shall be established in accordance with the following:
 - (a) considering that a margin in line with Article 22 of the CACM Regulation shall be taken into account for capacity calculation processes, and that the goal of the operational security analysis is to identify expected operational security limit violations and consequent remedial actions, each TSO shall not include any reliability margin to its operational security limits or in the coordinated operational security analysis;
 - (b) individual grid models and subsequent common grid models, created in the application of Article 70(2) of the SO Regulation and according to the methodology of Article 70(1) of the SO Regulation, shall include:
 - (i) load and intermittent generation forecasts established on the basis of the latest available forecasts for load and intermittent generation according to Article 37 and Article 38; and
 - (ii) market results, schedules, and planned topology of the transmission system;
 - (c) remedial actions shall be included in individual grid models and subsequent common grid models as required in Article 20Article 21 and Article 21.
2. The coordinated operational security analysis referred to in paragraph 1 shall be performed in accordance with Articles 72(1)(c), 74(1) and (2) of the SO Regulation, between T1 and T5 on the basis of the day-ahead common grid model built in accordance with Article 33(1), where T1 and T5 are defined in accordance with Article 45.
3. Each TSO shall have the right to delegate this task to the RSC(s) to which it has delegated tasks in accordance with Article 77(3) of the SO Regulation, while the TSO shall keep the legal responsibility of this task.

¹ Commission Regulation (EU) 2016/1719 of 26 September establishing a guideline on forward capacity allocation

Methodology for coordinating operational security analysis

4. When preparing the proposal for the common provisions for regional operational security coordination as required by Article 76 of the SO Regulation, all TSOs of a CCR shall have the right to establish particular rules and processes, applicable in day-ahead to the coordinated operational security analyses performed by these TSOs and the coordinated regional operational security assessments performed by the RSCs. Where they are needed to manage the exceptional situations where the accuracy of one or more of the forecasts variables included in the individual grid models is insufficient to allow the correct identification of operational security limit violations by application of paragraph 1. These rules and processes shall ensure that, when they are activated, all affected TSOs and RSCs, including those not involved in the proposal, are informed and can take account of these activations in their own processes.

Article 24

Intraday operational security analysis

1. Each TSO shall determine the minimum number and hours of assessment runs in intraday timeframe where it performs a coordinated operational security analysis in accordance with Article 72(1)(d), 74(1) and (2) of the SO Regulation, taking into account at least:
 - (a) conditions and frequency for coordinated regional operational security assessment provided by an RSC and adopted pursuant to Article 76(1)(a) of the SO Regulation in the capacity calculation regions the TSO is taking part;
 - (b) intraday relative timeline distribution of the market activity affecting the positions of market participants in its control area;
 - (c) time needed to activate remedial actions;
 - (d) impact of solar or wind generation variations on its system, due to locally connected generation assets or connected inside other control areas;
 - (e) impact of load variations.
2. The minimum number shall be greater than or equal to three.
3. Each TSO shall perform the coordinated operational security analyses as required in paragraph 1 on the basis of a best forecast approach, where the forecasted situation of each timestamp in the intraday timeframe shall be established in accordance with the following:
 - (a) considering that a margin in line with Article 22 of the CACM Regulation shall be taken into account for capacity calculation processes, and that the goal of the operational security analysis is to identify expected operational security limit violations and consequent remedial actions. Each TSO shall not add any reliability margin to its operational security limits or in the coordinated operational security analysis;
 - (b) individual grid models and subsequent common grid models, created in the application of Article 70(2) of the SO Regulation and according to the methodology of Article 70(1) of the SO Regulation, shall include load and intermittent generation forecasts. They shall be established on

Methodology for coordinating operational security analysis

- the basis of the latest available forecasts for load and intermittent generation according to Article 37 and Article 38;
- (c) individual grid models and subsequent common grid models, created in the application of Article 70(2) of the SO Regulation and according to the methodology of Article 70(1) of the SO Regulation, shall include market results, schedules, and planned topology of the transmission system;
 - (d) remedial actions shall be included in individual grid models and subsequent common grid models as required in Article 20Article 21 and Article 21Article 20.
4. When performing a coordinated operational security analysis in intraday, and where the results of the coordinated operational security analysis have significantly evolved with a regional impact compared to the previous ones, the TSO shall coordinate with the affected TSOs in accordance with Article 72(5) of the SO Regulation and the relevant RSC(s), in order to:
 - (a) share information about the significant changes of results, at least flows;
 - (b) agree on change of previously-agreed remedial action or on new remedial actions with cross-border relevance which may become required due to moving closer to or exceeding the operational security limits.
 5. With respect to the conditions and frequency of intraday coordination of operational security analysis established pursuant to Article 76(1)(a) of the SO Regulation, the TSO shall have the right to delegate part or all of the coordinated operational security analyses defined in accordance with paragraph 1 to the RSC(s) to which it has delegated tasks in accordance with Article 77(3) of the SO Regulation, while the TSO shall keep the legal responsibility of these tasks.
 6. When preparing the proposal for the common provisions for regional operational security coordination as required by Article 76 of the SO Regulation, all TSOs of a CCR shall have the right to establish particular rules and processes, applicable in intraday to the coordinated operational security analyses performed by these TSOs and the coordinated regional operational security assessments performed by the RSCs. Where they are needed to manage the exceptional situations where the accuracy of one or more of the forecasts variables included in the individual grid models is insufficient to allow the correct identification of operational security limit violations by application of paragraph 3. These rules and processes shall ensure that, when they are activated, all affected TSOs and RSCs, including those not involved in the proposal, are informed and can take account of these activations in their own processes.

Article 25 **Handling of extreme event**

1. In case of an expected extreme event, such as an extreme weather event, able to trigger significant effects on network assets' or generation assets' availability or on load demand, each TSO shall evaluate the expected consequences within its control area. The focus shall be on the period of the day from the moment where the event will take place until the end of the day.

Methodology for coordinating operational security analysis

2. Where the result of this analysis is that such an event is possibly leading to an emergency or black-out state, the TSO shall inform without undue delay neighbouring TSOs and the relevant RSC(s), and, where necessary, affected DSOs and SGUs.

Chapter 5
Cross-regional coordination

Article 26
General requirements

1. RSCs shall use English for all communication and documentation exchanges between them.
2. RSCs shall aim at providing permanent capability for coordination with other RSCs twenty-four seven. Where an RSC is not organised for that, a back-up solution shall be defined by the RSC and its delegating TSOs to allow possible exchange of information at the request of other RSCs during the periods when this RSC is unavailable.

Article 27
Overlapping zones, XNEs and XRAs

1. Where a network element has been defined as cross-border relevant in two or more different CCRs and where the physical flows on this XNE are significantly impacted by flows from electricity exchanges or activation of XRA in two or more CCRs, this XNE shall be defined as overlapping XNE. Such XNEs shall be grouped into overlapping zones and the concerned CCRs shall be considered as impacting CCRs for these overlapping zones.
2. The operational security violations on the overlapping XNEs shall be addressed first in one or more impacting CCRs at a regional level, and subsequently, the residual operational security violations, resulting after each regional operational security assessment is finalised, shall be addressed with a common cross-regional coordination process involving TSOs and RSCs of all impacting CCRs.
3. No later than eighteen months after the adoption of this methodology, all TSOs shall jointly develop a proposal for amendment of this methodology in accordance with Article 7(4) of the SO Regulation. The proposal shall complement this methodology with the following rules:
 - (a) rules for the identification and definition of overlapping XNEs, overlapping zones and impacting CCRs;
 - (b) rules for the identification of an impacting CCR and the competent RSC(s) that shall be responsible to first address operational security violations on overlapping XNEs at a regional level or, in case of shared responsibility, for defining the share of the operational security violation to be addressed by each impacting CCR and corresponding competent RSC(s) at a regional level;

Methodology for coordinating operational security analysis

- (c) rules for the identification of overlapping XRAs that may be used to address residual operational security violations as referred to in paragraph 2;
 - (d) the principles and rules for consistent interaction between coordinated regional and cross-regional operational security assessments and the rules for the identification of the most economically efficient remedial actions to address residual operational security violations at cross-regional level; and
 - (e) rules for the sharing of costs of the overlapping XRAs activated to address the residual operational security violations by assigning the shares of costs to individual overlapping XNEs and to individual impacting CCRs.
4. The rules pursuant to point (a) of paragraph 3 shall be based on objective and coordinated identification of the contributions of physical flows originating from different impacting CCRs, as well as, the criteria and threshold(s) above which the contribution of an impacting CCR is considered significant.
 5. The rules pursuant to point (b) of paragraph 3 shall specify, *inter alia*, that the operational security violations on the overlapping XNEs shall be addressed at the regional level first. This shall be done either by the TSOs and RSC(s) of an impacting CCR, which has the highest contribution to the physical flows on such overlapping XNE or by the TSOs and RSC(s) of two or more impacting CCRs in proportion to the historical or expected contribution of a given impacting CCR to the physical flows on such overlapping XNE.
 6. The rules pursuant to point (c) of paragraph 3 shall be consistent with the rules established in Article 15(3) to (8).
 7. The principles and rules pursuant to point (d) of paragraph 3 shall describe how the coordinated cross-regional operational security assessment will interact with coordinated regional operational security assessments and how the identification of the most economically efficient remedial actions to address residual operational security violations at cross-regional level shall be performed.
 8. The rules pursuant to point (e) of paragraph 3 shall specify, *inter alia*,:
 - (a) the rules to identify the costs of overlapping XRAs activated to address residual operational security violations on overlapping XNEs and to attribute these costs to individual overlapping XNEs, which shall be consistent with the regional rules for sharing the costs of remedial actions established in accordance with Article 76(1)(b)(v) of the SO Regulation and Article 74(1) of the CACM Regulation;
 - (b) the rules to identify the share of the costs attributed to individual overlapping XNEs that shall be attributed to each of the concerned impacting CCR. These rules shall be based on the shares of physical flows on the overlapping XNEs originating from different impacting CCRs and shall be consistent to the degree possible with the regional rules for sharing the costs of remedial actions established in accordance with Article 76(1)(b)(v) of the SO Regulation and Article 74(1) of the CACM Regulation.

Methodology for coordinating operational security analysis

9. When an XRA is identified as overlapping XRA in application of the rules pursuant to point (c) of paragraph 3, the XRA connecting TSO(s) shall provide to all RSCs of the concerned impacting CCRs the information about such XRA in accordance with Article 78(1) of the SO Regulation and shall decide on a single impacting CCR to which it shall provide such remedial action. This decision shall take account of the assumptions on remedial actions considered in capacity calculation methodologies established pursuant to Articles 20 and 21 of the CACM Regulation.
10. In the implementation of Articles 78, 80 and 81 of the SO Regulation, RSCs and TSOs shall take into account the agreements reached in accordance with paragraphs 1 to 8.

Article 28

Monitoring of inclusion of agreed remedial actions in the individual grid models

1. Each RSC shall monitor in the relevant timeframes the correct inclusion of the agreed remedial actions in the IGMs by the TSOs, as required by Article 70(4) of the SO Regulation.
2. When a RSC identifies that a previously agreed remedial action has not been included in the IGM by a TSO, that RSC shall inform the other relevant RSCs about it. The RSC in charge of CGM building for this TSO according to Article 77(3)(b) of the SO Regulation shall, in accordance with Article 79(3) of the SO Regulation, ask the relevant TSO to correct its IGM without undue delay.

Article 29

Back-up for the common grid model building task

1. RSCs shall set up the relevant organisation between them to guarantee the availability of common grid models built in application of Article 79 of the SO Regulation with a target of absence of interruption for the different timeframes.
2. In case of an interruption of service, RSCs shall aim at recovering the service availability as soon as possible and inform the TSOs of the expected time of recovery.

Article 30

Coordinated cross-regional operational security assessment

1. Coordinated cross-regional operational security assessment shall be performed for overlapping XNEs within the overlapping zones defined pursuant to Article 27.
2. Residual operational security violations on overlapping XNEs within the overlapping zones, remaining after the coordinated regional operational security assessment in accordance with Article 78 of the SO Regulation, shall be addressed with a common cross-regional coordination process involving the TSOs and RSC(s) of the impacting CCRs. In this process, the RSCs shall coordinate to find the most effective and economically efficient overlapping XRAs to be proposed to their TSOs to address residual operational security limit violations on overlapping XNEs within the overlapping

Methodology for coordinating operational security analysis

zones. The competent RSCs shall ensure that this process does not create new operational security limit violations.

3. After defining the optimal overlapping XRA to address residual operational security violations on overlapping XNEs, the concerned TSOs shall identify the costs of such overlapping XRA and attribute a share of these costs to each individual overlapping XNE. The share of costs attributed to each overlapping XNE shall be further shared among the concerned CCRs first, in application of the rules pursuant to Article 27(3)(d), and subsequently among the TSOs of each CCR according to the regional rules for sharing the costs of remedial actions established in accordance with Article 76(1)(b)(v) of the SO Regulation and Article 74(1) of the CACM Regulation.

Article 31

Investigation of possible additional remedial actions

1. When a RSC is not able to propose to its delegating TSOs effective and economically efficient remedial actions to remove a violation of operational security limits, this RSC shall coordinate with other relevant RSCs in order to try to find another possible remedial action to remove it. When doing so, RSCs may recommend remedial actions other than those provided by the TSOs in accordance with Article 78(2)(a) of the SO Regulation.

Article 32

Exchange of results

1. Each RSC shall exchange the results of coordinated regional operational security assessments with other RSCs, when having an overlapping zone with it, for checking and consolidating them where required, notably for cross-regional operational security assessment. They shall at least exchange information about needed remedial actions and all relevant information useful to support the results.

Article 33

Regional and cross-regional day-ahead coordinated operational security assessment

1. TSOs and RSCs shall apply at least the following regional and cross-regional day-ahead coordinated operational security assessment process, where T0, T1, T2, T3, T4, T5 are defined in accordance with Article 45:
 - (a) at the latest at hour T0, all TSOs shall deliver IGMs covering the whole next day and RSCs shall make available to all TSOs and RSCs the corresponding CGMs before hour T1 where T1 is equal to T0 +60 minutes, in accordance with Article 22(4)(d) of the methodology established pursuant to Article 70(1) of the SO Regulation;
 - (b) at the latest at hour T2, each RSC shall perform a coordinated regional operational security assessment as required by Article 78(2) of the SO Regulation;

Methodology for coordinating operational security analysis

- (c) at the latest at hour T2, RSCs shall share between them the results of these coordinated regional operational security assessments. Between T2 and T3, TSOs shall deliver updated IGMs taking into account the preventive remedial actions agreed during this coordinated regional operational security assessment, and making also available the curative remedial actions agreed during this coordinated regional operational security assessment;
 - (d) at the latest at hour T3, RSCs shall make available to all TSOs and RSCs the corresponding CGMs in accordance with Article 22(4)(e) of the methodology established pursuant to Article 70(1) of the SO Regulation;
 - (e) at the latest at hour T4, each RSC shall perform a coordinated cross-regional operational security assessment as required by Articles 78(2) and (3) of the SO Regulation on the basis of the CGMs established in accordance with paragraph ((d)), including where relevant analysing the use of additional remedial actions pursuant to Article 30(2) and Article 31;
 - (f) between T4 and T5, RSCs shall organise a session, such as a teleconference, where the results of coordinated regional operational security assessments performed according to paragraph (e) and proposed remedial actions are shared. During this session, TSOs and RSCs shall consolidate the final outcomes of the whole process described in paragraphs (a) to (e), and TSOs shall agree on the remedial actions, in application of Article 78(4) of the SO Regulation. Each TSO shall participate in this session or shall appoint its RSC to represent it at the session while the TSO keeps the legal responsibility to agree on remedial actions;
 - (g) each TSO shall include the agreed remedial actions in accordance with paragraph ((f)) in their first intraday IGMs to be provided after T5 in accordance with the requirements of the methodology developed according to Article 70(1) of the SO Regulation.
2. During this process, RSCs and TSOs may have additional exchanges needed to facilitate its effectiveness.
 3. Later in intraday, when RSCs perform coordinated regional operational security assessments or TSOs perform coordinated operational security analyses, they shall take the cross-regional day-ahead coordinated operational security assessment's final outcomes and agreed remedial actions as a reference basis, against which needed adaptations shall be assessed.
 4. Where violations of operational security limits remain at the end of the cross-regional day-ahead coordinated operational security assessment process, the concerned TSOs and RSCs shall agree on the objectives and the needed steps to follow in intraday, in order to improve the management of these remaining violations.
 5. When paragraph 4 applies, the concerned RSCs shall record the event and the outcome of the intraday activity to manage these remaining violations after the cross-regional day-ahead coordinated operational security assessment process, and shall report this information in the report prepared in accordance with Article 17(2) of the SO Regulation.

Article 34

Intraday coordinated regional operational security assessment

1. RSCs shall aim at synchronising the timing of the processes for the coordinated regional operational security assessments they perform in accordance with Article 78 of the SO Regulation, for harmonised time frames in intraday, taking into account the approved proposals set up by TSOs in the different capacity calculation regions in accordance with Article 76(1) of the SO Regulation.

Article 35

Outage planning coordination tasks

1. In application of Articles 80(4) and 80(5) of the SO Regulation, when a RSC and its delegating TSOs have not succeeded to remove an outage planning incompatibility, this RSC shall coordinate with other RSCs to endeavour to propose cross-regional solutions to remove the incompatibility.

Article 36

Regional adequacy assessment tasks

1. RSCs shall define a process in order to strengthen the regional adequacy assessment performed by each RSC as required by Article 81 of the SO Regulation, by identifying the capabilities of further support between regions, for at least the time frame of week-ahead and for other agreed time frames.
2. This process shall at least ensure that RSCs exchange information on available generation capacity, demand and interconnection capacities in each region, when performing regional adequacy assessment as required by Article 81 of the SO Regulation.

TITLE 4

Forecast updates with respect to uncertainty management

Chapter 1

Forecasts

Article 37

Forecast of intermittent generation

1. Each TSO shall consider the following criteria in establishing forecasts of intermittent generation in accordance with paragraphs 2 to 5:
 - (a) the forecasts established shall cover at least the control area of the TSO, including intermittent generation located in underlying DSO/CDSO networks, and shall be complemented where necessary in accordance with paragraph b;
 - (b) each TSO shall evaluate if there are cases where the installed intermittent generation in specific geographical regions within its control area are such that it would be insufficient to establish

Methodology for coordinating operational security analysis

- forecasts at control area level only. Where such cases are identified the TSO shall determine an appropriate frequency of forecast for the intermittent sources within the identified geographical region such that deviations from the forecast would not endanger the operational security of the interconnected system or the efficient system operation;
- (c) the requirements of paragraphs 2 to 5 shall be considered as minimal requirements and each TSO shall assess whether the accuracy of the resulting forecasts is sufficient in application of Articles 70(4) and 70(5) of the SO Regulation.
2. Where total wind (resp. total solar) installed capacity is between 1% and 10% of the reference load, each TSO shall ensure the availability of at least one wind (resp. solar) generation forecast in day-ahead for each hour of the day of delivery. It must be established after weather forecast has been made available.
 3. Where total wind (resp. total solar) installed capacity is between 10% and 40% of the reference load:
 - (a) each TSO shall ensure the availability of an update of the wind (resp. solar) hourly forecast at least 2 times per day in intraday, based on at least 2 weather forecast updates;
 - (b) in cases where total wind and total solar installed capacities each are above 10% of the reference load, and the sum of the total installed capacity of wind and solar is above 40%, each TSO shall ensure the availability of an update of the wind and solar forecast for each hour of the day at least 2 times per day in intraday, based on at least 2 weather forecast updates and using the best available estimation of actual generation after having qualified that it allows to improve forecast accuracy, compared to the accuracy resulting of requirement of point (a) of paragraph 3.
 4. Where total wind (resp. total solar) installed capacity is above 40% of the reference load, each TSO shall ensure the availability of an update of the wind (resp. solar) forecast for each hour of the day at least 2 times per day in intraday, based on at least 2 weather forecast updates and using the best available estimation of actual generation after having qualified that it allows to improve forecast accuracy, compared to the accuracy resulting of the application of requirement of point (a) of paragraph 3.
 5. Where another type of intermittent generation installed capacity, such as run of river hydro generation, is above 1% of the reference load, each TSO shall ensure the availability of least one forecast for this generation type, established in day-ahead for each hour of the day of delivery.

Article 38

Forecast of load

1. Each TSO shall consider the following criteria in establishing forecasts of load in accordance with paragraphs 2 to 3:
 - (a) the forecasts established shall cover at least the control area of the TSO, including the load of underlying DSO/CDSO networks and shall be complemented where necessary in accordance with paragraph (b)1;
 - (b) each TSO shall evaluate if there are cases where load and network conditions in specific geographical regions within its control area would make it insufficient to establish forecasts at

Methodology for coordinating operational security analysis

- control area level only. Where such cases are identified, the TSO shall determine an appropriate frequency of forecast for the load within the identified geographical region such that deviations from the forecast would not endanger the operational security of the TSO's system;
- (c) where aspects, such as demand response or energy storage, may affect the load forecast, each TSO shall ensure that the effects of these factors are considered in the forecasts;
 - (d) the requirements of paragraphs 2 to 3 shall be considered as minimal requirements and each TSO shall assess whether the accuracy of the resulting forecasts is sufficient in application of Articles 70(4) and 70(5) of the SO Regulation.
2. Each TSO shall ensure the availability in day-ahead of one load forecast per hour for every day, using the best information available in day-ahead.
 3. Without prejudice to the application of Article 40(5) of the SO Regulation, for a control area where the MW/°C gradient is greater than 1% of the reference load, the TSO shall ensure the availability of at least one load forecast per hour for all the day of delivery, based on a weather forecast established at least in the afternoon of the day before the day of delivery. For the control area, the TSO shall establish at least one update in intraday between 0h and 12h for the remaining hours of the day of delivery.

Chapter 2

Grid model updates in intraday

Article 39

Frequency of grid model updates

1. By 1 January 2023, and then at least every three years, all TSOs shall assess the need to review the individual grid models and common grid models intraday update frequency as defined in the methodology developed according to Article 70(1) of the SO Regulation. They shall take into account the expected evolution of volatile parameters, such as market positions, intermittent generation and load.

TITLE 5

Governance and implementation

Chapter 1

Governance

Article 40

Identification and governance of common functions and tools

1. All TSOs, with the support of the RSCs, shall aim at regularly identifying the common functions and tools needed for a secure and efficient system operational planning and the relevant information that need to be exchanged among them, at least to implement the tasks listed in Articles 78, 79, 80 and 81 of the

Methodology for coordinating operational security analysis

SO Regulation. The functions, tools, and relevant information to be identified shall be of pan-European use or of regional use.

2. For the functions and tools and relevant information identified in accordance with paragraph 1, as well as for those needed to implement the common grid model building task defined in Article 79 of the SO Regulation and the operational planning data environment defined in Article 114 of the SO Regulation, all relevant TSOs, with the support of the RSCs, using, where deemed useful, ENTSO-E bodies, resources and budget and, in that case, in accordance with the provisions of ENTSO-E articles of association, shall:
 - (a) decide on their development;
 - (b) provide the needed budgets for their development and maintenance;
 - (c) agree on the rules applicable for the management of the development and maintenance, including evolutions;
 - (d) agree on the applicable process to select the hosting entities for their operation, notably in terms of competence and resources necessary to achieve the needed levels of reliability, confidentiality and security;
 - (e) and agree on the characteristics of the service delivered by these functions and tools.
3. To facilitate the development and operation of functions and tools identified in accordance with paragraph 1, all TSOs, using, where deemed useful, ENTSO-E bodies and resources, in accordance with the provisions of ENTSO-E articles of association, shall aim at using or defining state-of-the-art standards for project management, data exchange and IT common services.

Article 41

Coordination and information exchange with regional security coordinators

1. All TSOs shall enable all RSCs to execute their tasks delegated in accordance with Articles 77(3), 77(4) and 77(5) of the SO Regulation and provide them with all necessary data.
2. All RSCs shall share with each other all data relevant for the execution of their tasks in accordance with Articles 77(3), 77(4) and 77(5) of the SO Regulation.
3. All TSOs shall duly consider Article 75(1)(d) of the SO Regulation when defining the requirements applicable to the RSCs and the merging process in accordance with Article 23 of the methodology on common grid model pursuant to Article 70(1) of the SO Regulation.
4. All TSOs shall enable all RSCs to assess the impact across CCRs and the impact across RSCs when:
 - (a) designing remedial actions in accordance with Article 78(2) of the SO Regulation;
 - (b) recommending remedial actions in accordance with Article 78(2) of the SO Regulation;
 - (c) conducting regional outage coordination in accordance with Article 80 of the SO Regulation;
 - (d) conducting regional adequacy assessment in accordance with Article 81 of the SO Regulation.

Methodology for coordinating operational security analysis

5. RSCs shall assess the impact across CCRs and across RSCs and inform the relevant TSOs about this impact.

Article 42

Data quality assessment

1. By 1 January 2023, and then at least every three years, for the functions and tools and relevant information identified in accordance with Title 4, all relevant TSOs and RSCs, shall define data quality management provisions for the data exchanged in this process. The provisions shall be developed at least to the same level of detail as the quality monitoring criteria and indicators defined pursuant to Article 2323 of the common grid model methodology adopted in accordance with Article 70 of the SO Regulation.
2. Where such a need is identified, all relevant TSOs and RSCs shall:
 - (a) define the data quality criteria, the process to check that the criteria are satisfied before using the data and the process for monitoring data quality criteria achievement;
 - (b) identify, using where deemed useful ENTSO-E bodies and resources, a common body in charge of analysing results of the data quality monitoring, reviewing the level of quality needed, and preparing when relevant the revisions of the data quality criteria.

Article 43

Monitoring of regional coordination

1. All TSOs, with the support of ENTSO-E bodies and resources, shall organise at least every three years an inquiry towards TSOs and RSCs, in order to collect their evaluation of the appropriateness and efficiency of the processes and rules applied for the coordination of the operational security analyses, outage coordination and short and medium term adequacy analyses in the operational planning time frame. This inquiry shall allow all TSOs to establish conclusions and identify, if any, improvement perspectives in terms of:
 - (a) data quality, including the quality of forecasts of generation, load and remedial actions in accordance with Titles 3 and 4;
 - (b) efficiency and adaptation of processes to day-ahead or intraday activities, and flexibility to handle out-of-procedure situations;
 - (c) availability of remedial actions to solve system security issues in a coordinated way, where a coordinated approach is relevant;
 - (d) existing barriers to coordination.
2. When defining the scope of this inquiry, in order to keep the inquiry process efficient, all TSOs and RSCs shall take account of information and conclusions made in the reports established in accordance with Article 17 of the SO Regulation.
3. The conclusions of this inquiry shall be published on ENTSO-E's website. ENTSO-E shall inform the Agency for the Cooperation of Energy Regulators of this publication and each TSO shall inform its regulatory authority.

Methodology for coordinating operational security analysis

4. If this inquiry reveals the need to amend this methodology, all TSOs shall amend this methodology accordingly by following the process pursuant to Article 7(4) of the SO Regulation.

Article 44

Towards probabilistic risk assessment

1. All TSOs shall publish, with the support of ENTSO-E, a report on the progress achieved in Europe on the operational probabilistic coordinated security assessment and risk management. The first report shall be published in 2021 and afterwards on a biennial basis, by 31 December. ENTSO-E shall publish this report on its website.
2. When reporting on the progress achieved, all TSOs shall at least:
 - (a) provide information on the functioning of the operational processes and infrastructure required to collect and process the data referred to in paragraph 3; and
 - (b) elaborate on the achievements, potential hurdles and forward planning concerning the development of the methodology on common probabilistic risk assessment referred to in paragraph 4.
3. By nine months after the adoption of the CSAM, without prejudice to the application of Article 40(5) of the SO Regulation, all TSOs shall identify the data that needs to be collected in order to develop the operational probabilistic coordinated security assessment and risk management. They shall review it as necessary based on the findings of the reports established in accordance with paragraphs 1 and 2 and of the approval of the methodology on common probabilistic risk assessment in accordance with paragraph 4.
4. By 31 December 2027, all TSOs shall jointly develop the methodology on common probabilistic risk assessment taking full account of the requirements of Article 75(1)(b) and Article 75(5) of the SO Regulation, and shall propose it as an amendment of this methodology in accordance with Article 7(4) of the SO Regulation. After its approval in accordance with Article 7 of the SO Regulation, the methodology on common probabilistic risk assessment shall form an annex to this methodology.
5. All TSOs and RSCs with the support of ENTSO-E shall setup the operational processes and infrastructure required to collect and process the data referred to in paragraph 2(b) by 21 months after the adoption of the CSAM.

Chapter 2

Implementation

Article 45

Definition of common hours

1. By three months after the approval of this methodology, all TSOs, with the support of all RSCs, shall jointly define the hours T0 to T5. ENTSO-E shall publish these hours on its website.

Methodology for coordinating operational security analysis

2. As long as ENTSO-E has not published these hours, the following 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.
3. All TSOs shall assess every three years by 1 July the adequacy of the cross-regional day-ahead coordinated operational security assessment process as defined in Article 33 to the needs. This assessment shall be submitted to the Agency for the Cooperation of Energy Regulators and all regulatory authorities. They shall at least analyse the opportunities to start earlier and to reduce the total duration of the process clearly listing any barriers for starting earlier and reducing the total length of the process. The result of the first assessment shall be reported no later than 24 months after approval of this methodology.

Article 46

Timescale for implementation

1. Upon approval of this methodology, each TSO shall publish it on the internet in accordance with Article 8(1) of the SO Regulation.
2. After approval of this methodology, and unless differently stipulated in the previous articles or in the following paragraphs of this article, each TSO and RSC shall apply the requirements of this methodology within six months after its approval.
3. Each TSO shall apply the requirements of Article 37 and Article 38 within 12 months after approval of this methodology.
4. RSCs and their delegating TSOs concerned by the application of the requirements of Article 27 shall establish the elements defined in paragraph 1 and 2 by six months after the submission of the proposal(s) to be developed by the corresponding TSOs in application of Articles 76 and 77 of the SO Regulation.
5. No later than six months after the RSC task pursuant to Article 78 of the SO Regulation has been implemented for its delegating TSOs, in application of the approved proposal of these TSOs as required by Articles 76 and 77 of the SO Regulation, the concerned RSCs and these TSOs shall participate to the cross-regional day-ahead coordinated operational security assessment process in accordance with Article 33.
6. No later than six months after RSC tasks pursuant to Article 78 of the SO Regulation have been implemented in application of approved proposals as required by Articles 76 and 77 of the SO Regulation, concerned RSCs shall implement the requirements of Article 30, Article 31, and Article 32.
7. No later than twelve months after RSC tasks pursuant to Article 79 of the SO Regulation have been implemented in application of approved proposals as required by Articles 76 and 77 of the SO Regulation, concerned RSCs shall have implemented the relevant organisation between them to guarantee the availability of common grid models in accordance with Article 29.
8. No later than eighteen months after the adoption of this methodology, all TSOs shall jointly develop a proposal for amendment of this methodology with rules for the identification and definition of overlapping zones, overlapping XNEs, overlapping XRAs, impacting CCRs and competent RSC(s), as

Methodology for coordinating operational security analysis

well as, rules for the sharing of costs of the activated overlapping XRAs, in accordance with Article 27(3). The proposal shall include a timescale for the implementation of Article 27 and Article 30.

9. No later than six months after RSC tasks pursuant to Article 80 of the SO Regulation have been implemented in application of approved proposals as required by Articles 76 and 77 of the SO Regulation, concerned RSCs shall implement the requirements of Article 35.
10. No later than six months after RSC tasks pursuant to Article 81 of the SO Regulation have been implemented in application of approved proposals as required by Articles 76 and 77 of the SO Regulation, concerned RSCs shall implement the requirements of Article 36.
11. Each TSO shall apply the requirements of Article 5(1) and Article 6(1) by three months after approval of this methodology. In case the CGMs required by the Article 67 of the SO Regulation are not available when this methodology is approved, each TSO shall apply the requirements of these articles by three months after these CGMs are made available.
12. Each TSO shall apply Article 5(4), where applicable, by three months after receiving needed data from DSO/CDSOs according to Article 3(7).
13. Each TSO shall apply the requirements of Article 4, where applicable, by six months after receiving needed data from concerned TSOs, DSO/CDSOs and SGUs according to Article 4(5).
14. All TSOs shall report on opportunities to start earlier and to reduce the total length of the process on coordinated security analysis by 24 months after approval of this methodology, and then triennially by 1 July, in accordance with Article 45.
15. By 31 December 2027, all TSOs shall develop and submit, with the support of ENTSO-E, the methodology on common risk assessment taking full account of the requirements of Article 75(1)(b) and Article 75(5) of the SO Regulation in accordance with Article 44(4)

Article 47 **Language**

1. The reference language for the CSAM shall be English. Where TSOs need to translate the CSAM into their national language(s), in the event of inconsistencies between the CSAM and any version in another language, the relevant TSOs shall provide, in accordance with national legislation, the relevant regulatory authorities with an updated translation of the CSAM.

Annex I

AI.1 Influence threshold

Power flow influence factor is evaluated by computing two elementary factors: power flow identification influence factor and power flow filtering influence factor. These factors are defined in AI.2.

| Set of elements | Power flow identification influence threshold | Power flow filtering influence threshold | Voltage influence threshold |
|---------------------------|---|--|-----------------------------|
| Observability area | 5 – 10 % | 3 – 5% | 0.01 – 0.02 pu |
| External Contingency list | 15 – 25% | 3 – 5% | 0.03 – 0.05 pu |

AI.2 Influence Computation Method

In order to compute influence of system elements connected outside TSO's control area on its control area the following definitions have been introduced (Figure 1):

- Element t is a network element connected in TSO's control area and which is influenced by a system element connected outside TSO's control area;
- Element r is a network element connected outside TSO's control area whose influence is assessed;
- Elements i are network elements connected either in TSO's control area or outside TSO's control area which are disconnected to represent planned (or forced) outages.

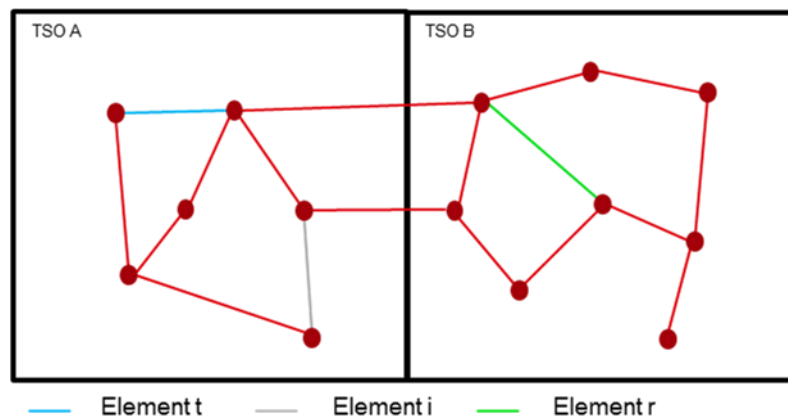


Figure 1

AI.2.1 Power flow influence factor

AI.2.1.1 Network elements

The influence of a network element (r) shall be assessed by each TSO using following formulae:

$$IF_r^{pf,id} (in \%) = MAX_{\forall i \in I, \forall s, \forall t \in T} \left(\frac{P_{s,n-i-r}^t - P_{s,n-i}^t}{P_{s,n-i}^r} \cdot \frac{PATL^{s,r}}{PATL^{s,t}} \cdot 100 \right)$$

$$IF_r^{pf,f} (in \%) = MAX_{\forall i \in I, \forall s, \forall t \in T} \left(\frac{P_{s,n-i-r}^t - P_{s,n-i}^t}{P_{s,n-i}^r} \cdot 100 \right)$$

Where

$IF_r^{pf,id}$: Power flow identification influence factor of a network element r on the TSO's control area; the factor is normalised in order to take into account potential impacts induced by differences in PATL values;

$IF_r^{pf,f}$: Power flow filtering influence factor of a network element r on the TSO's control area; this factor is not normalised;

s: Scenarios. Settings of HVDC systems and PSTs in the different scenarios are assumed to be already defined, in a coherent way, in the context of the scenarios/CGMs development process;

t: Network element connected inside TSO's control area where the active power difference is observed;

T: Set of network elements connected in the TSO's control area, which are part of the CGM and for which the assessment is performed;

i: Network element connected either in TSO's control area or outside TSO's control area (different from elements r and t) considered disconnected from the network when assessing the formula;

I: Set of network elements, connected either in TSO's control area or outside TSO's control area, modelled in the grid model whose possible outage should be taken into account in the assessment;

r: Network element connected outside TSO's control area whose power flow influence factor is assessed;

R: Set of network elements connected outside TSO's control area to be assessed;

P_{n-i}^t : Active power flow through the network element t with the network element r connected to the network and the network element i disconnected from the network;

P_{n-i}^r : Active power flow through the network element r, when connected to the network, considering the network element i disconnected from the network;

P_{n-i-r}^t : Active power flow through the network element t with the network element r and the network element i disconnected from the network;

$PATL^{s,t}$: Permanently Admissible Transmission Loading is the loading in MVA or MW that can be accepted by network element t in the scenario s for an unlimited duration;

$PATL^{s,r}$: Permanently Admissible Transmission Loading is the loading in MVA or MW that can be accepted by network element r in the scenario s for an unlimited duration.

Methodology for coordinating operational security analysis

NB: Those computations have to be done inside one synchronous area. By principle, $IF_r^{pf,id}$ and $IF_r^{pf,f}$ are equal to 0 when r and t are not located in the same synchronous area.

The formulae must be applied, for each network element r which belongs to the set R, assessing its influence on every network element t of the TSO's control area for which the assessment is performed, and considering possible outages (network element i) (Figure 1).

The influence factor of an element connected in a given synchronous area on another element connected in a different synchronous area shall be equal to 0. Outages of HVDC links inside a synchronous area are treated as outages of AC elements.

Each TSO shall classify an 'r' element as selected for a given type of influence factor computation (observability area or external contingency) when the following conditions are simultaneously satisfied:

Power flow identification influence factor > Chosen-threshold1
Power flow filtering influence factor > Chosen-threshold2

where Chosen-threshold1 and Chosen-threshold2 are uniquely chosen by the TSO inside the ranges provided above in AI.1

AI.2.2 Voltage influence factor

If a TSO decides to use voltage influence factors in the determination of the aforementioned lists (observability area or external contingency) the influence of a network element r shall be assessed using the following formula:

$$IF_r^v = \text{MAX}_{\forall s, \forall m(m \in M)} \left(\left| \frac{V_{s,n-1}^{m,r} - V_{s,n}^m}{V_{base}^m} \right| \right)$$

Where:

IF_r^v : Voltage influence factor of a network element r on a node m of the TSO's control area;

s : Scenarios. Settings of HVDC systems and PSTs in the different scenarios are assumed to be already defined, in a coherent way, in the context of the scenarios/CGMs development process;

r : Network element connected outside TSO's control area whose voltage influence factor is assessed;

R : Set of network elements connected outside TSO's control area to be assessed;

$V_{s,n-1}^{m,r}$: Voltage at node m with the network element r disconnected from the network;

$V_{s,n}^m$: Voltage at node m with the network element r connected to the network;

V_{base}^m : Nominal voltage in the node m .

The formula must be applied, for each network element r that belongs to the set R , assessing its influence on every node m of the TSO's control area. The voltage influence factor of a network element r is the maximum value of the previous calculations.

Hence, the influence factor on voltage is the maximum Voltage Deviation on any internal node m resulting from the outage of a network element r in any scenario. For sake of simplicity, voltage is expressed in per unit. Contrary to the influence of flows, the influence on voltage of a network element is highly dependent on the load/generation pattern i.e. the active and reactive load of the network element in the investigated scenarios.

Where a TSO intends to use voltage influence factors, the TSO shall classify a 'r' element as selected for a given type of influence factor computation (observability area or external contingency) when the following condition is satisfied:

Voltage influence factor > Chosen-threshold

where Chosen-threshold is uniquely chosen by the TSO inside the ranges provided above in AI.1