Supporting document to the all TSOs' proposal for the 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 and for the methodology for assessing the relevance of assets for outage coordination in accordance with Article 84 of the same Regulation

10 July 2018

Disclaimer

This explanatory document is provided by all Transmission System Operators (TSOs) for information purposes only and accompanying the all TSOs' proposal for the 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 and for the methodology for assessing the relevance of assets for outage coordination in accordance with article 84 of the same Regulation.

ENTSO-E AISBL • Avenue de Cortenbergh 100 • 1000 Brussels • Belgium • Tel + 32 2 741 09 50 • Fax + 32 2 741 09 51 • info@entsoe.eu • www. entsoe.eu

Contents

1. Introduction

The Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation (hereinafter "**SO GL**") was published in the official Journal of the European Union on 25 August 2017 and entered into force on 14 September 2017. The SO GL sets out guidelines regarding requirements and principles concerning operational security, as well as the rules and responsibilities for the coordination between TSOs in operational planning. To deliver these objectives, several steps are required.

One of these steps is the development of the methodology for coordinating operational security analysis in accordance with article 75 of the SO GL (hereinafter "**CSAM**"), and the methodology for assessing the relevance of assets for outage coordination in accordance with article 84 (hereinafter "**RAOCM**"), 12 months after entry into force of the SO GL. CSAM and RAOCM are subject to public consultation in accordance with article 11 of the SO GL.

This supporting document has been developed in recognition of the fact that the CSAM and the RAOCM, which will become legally binding documents after NRAs' approval, inevitably cannot provide the level of explanation, which some parties may desire. Therefore, this document aims to provide interested parties with the background information and explanation for the requirements specified in the CSAM and the RAOCM.

The supporting document provides explanations developed in the following chapters:

- Chapter 2-Roles and organisation of security analyses: this is a transversal part
- Chapter 3-Influence: this chapter is linked to requirements provided in Art 75(1)(a) and Art 84 of SO GL
- Chapter 4-Risk Management: this chapter is linked to requirements provided in Art 75(1)(b); it also provides additional elements which are linked to those provided in Chapter 2
- Chapter 5-Uncertainties: this chapter is linked to requirements provided in Art 75(1)(c)
- Chapter 6-RSC coordination: this chapter is linked to requirements provided in Art 75(1)(d)
- Chapter 7-ENTSO-E role: this chapter is linked to requirements provided in Art 75(1)(e)

Additionally, a cross-reference is available in Annex. This table reminds the detailed wording of articles of SO –GL linked to CSAM-RAOM and how they are addressed in CSAM or RAOM.

Link with other methodologies

CSAM and RAOCM are also in relation with some other methodologies required by SO GL or the Commission Regulation (EU) 2015/1222 of 24 July 2015 establishing a guideline on capacity allocation and congestion management (hereinafter CACM). More precisely:

CSAM provides several requirements which are identified by TSOs as necessary to be harmonized at pan-European level and which shall be respected by the more detailed proposals set-up at CCR level, as requested by SO GL Art. 76-77. Such requirements concern:

- Identifying which remedial actions need to be coordinated, i.e. remedial actions which cannot be decided alone by a TSO but need to be agreed by other affected TSOs
- Identifying which congestions on which grid elements need to be solved at regional level under the coordination task delegated to a RSC, in accordance with SO GL Article 78
- Identifying which rules need to be applied to ensure inter-RSC coordination when RSCs provide their tasks to the TSOs,
- Requesting a minimum number of intraday security analyses to be done by a TSO (or delegated to its RSC)

Please note that the process for the management of the remedial actions in a coordinated way is not part of CSAM. This shall be developed by TSOs at CCR level in accordance with Art 76-77, while respecting the requirements set-up in CSAM.

CSAM also does not provide requirements to determine which remedial actions are of cross-border relevance and can be used to solve congestions which need to be solved at regional level; this is left to regional choice at CCR level when developing the proposal in accordance with Art 76-77 (and the proposal in accordance with Article 35 of CACM)

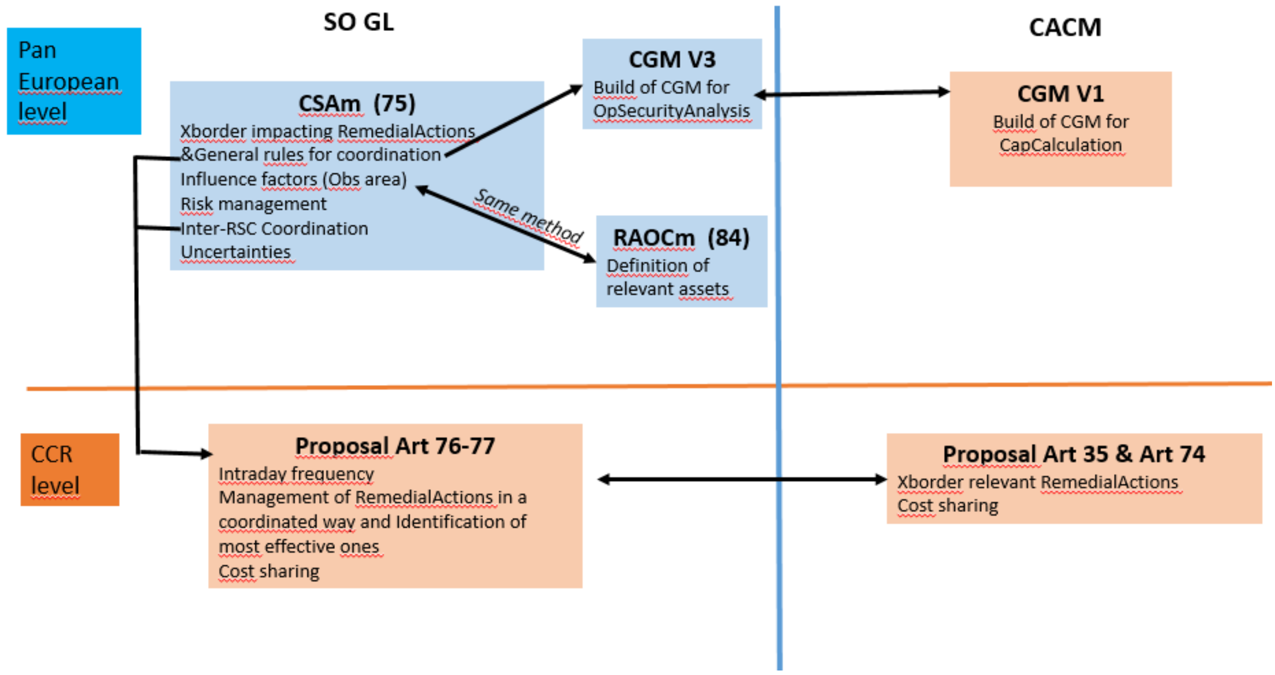
CSAM is also in relation with the all-TSOs methodology Common Grid Model V3 (CGMM V3) developed in accordance with SO GL Articles 67 and 70, as follows:

- CSAM provides requirements defining which remedial actions shall be included (or may be included) in an individual grid model (IGM), while CGMM defines how to include them in the IGMs, and then in the CGMs.
- CSAM defines timestamps in day-ahead (named T0 to T5) which are required for a proper inter-regional coordination in day-ahead, while some of these timestamps are used in the CGMM to define the process of building the IGMs and CGMs required by this coordination.

Additional links exist at regional level between:

- Proposals required by Art 76-77 of SO GL which deal with the management of the remedial actions in a coordinated way and Art 35 of CACM
- Proposals required by Art 76-77 of SO GL which deal with the cost sharing of the remedial actions managed in a coordinated way and Art 74 of CACM

Such links are summarized below (only main interactions are shown):


SO GL
CACM
Pan European level
CSAm (75)
Xborder impacting RemedialActions
&General rules for coordination
Influence factors (Obs area)
Risk management
Inter-RSC Coordination
Uncertainties
CGM V3
Build of CGM for OpSecurityAnalysis
CGM V1
Build of CGM for CapCalculation
Same method
RAOCm (84)
Definition of relevant assets
CCR level
Proposal Art 76-77
Intraday frequency
Management of RemedialActions in a coordinated way and Identification of most effective ones
Cost sharing
Proposal Art 35 & Art 74
Xborder relevant RemedialActions
Cost sharing

2. Roles and organisation of security analysis in operational planning

In the long term (year-ahead to week-ahead), operational security analyses are mainly focused on the outage planning process to ensure that these outages will be compatible with a secure operation and on the evaluation on general assessment of the expected security of the system in terms of expected congestion and adequacy. SO GL provides requirements to do these activities in a coordinated way, and CSAM/RAOCM provides for some additional rules (such as the determination of exceptional contingencies, the activities needed to facilitate the identification in the short term of remedial actions which need to be coordinated, the management of uncertainties in long-term studies…). Those rules are explained notably in the chapters Risk management and Uncertainties in this document.
In the short-term, mainly from day-ahead, operational security analyses mainly deal with the identification of risks on the interconnected system of operational security limits violations, trying to find the appropriate remedial actions, according to SO GL Article 21, and ensuring the coordination of these remedial actions.

These activities –long and short term- are also linked to the capacity calculation processes which determine capacities between bidding zones which can be offered to the market participants; those capacities are computed on the basis of a set of expectations. It's only when these expectations are verified in real time that the use of these capacities will respect the security of the system. As a result, at any moment ahead of real time, one of the roles of operational security analyses is to check that the positions taken by market participants are expected to be compatible with the system security, and if it is not the case, to prepare remedial actions.

According to SO GL, in long term as well in short term, coordinated security analyses are done on a common grid model in the operational planning phase.

The following chapter provides a focus on the realisation of security analyses in the short-term in order to facilitate the description of the security analyses done by TSOs and by RSCs in accordance with SO GL and CSAM and how they interfere between them. As such, this chapter 2 of the supporting document provide general information which is transversal to the different topics covered by CSAM and has notably interactions with chapter 4 "risk management", chapter 5 "Uncertainties" and chapter 6 "RSC coordination".

2.1 Types and chaining of security analyses in the short-term

Day-Ahead

TSOs identify that a very important step to assess security is at the end of D-1 and needs a well-coordinated sequential process, for the following reasons:

- the results of the Day-Ahead market are known,
- there exists still a relatively long period of time ahead of real time to allow in-depth studies and relatively complex processes, or to decide a remedial action which needs a long preparation time (such as starting a unit)
- planned outages are finalized and late forced outages can already be taken into account
- quite good forecasts for load and intermittent generation are available
- most of the contracted reserves (FCR, FRR, RR) have been allocated to their suppliers.

This process shall include regional coordination but also cross-regional coordination through RSCs coordination. This process shall allow:

- to design remedial actions in a coordinated manned at a regional level, using the agreed conditions pursuant to SO GL art 76-77,
- but also, to identify cross-regional effects of such remedial actions and ensure they are agreed by all affected TSOs,
- or, alternatively, when a congestion cannot be relieved using available remedial actions at regional level (or in an inefficient way), to elaborate cross-regional remedial actions able to relieve it.

It is the reason why the process described in Article 33 has been introduced in the CSAM. It is inspired of the current existing process between Coreso, TSCNet and their TSOs, with several improvements enhancing the inter-RSC coordination in order to ensure that potential remedial actions identified in one region are taken into account for their effects on the adjacent regions, before final remedial actions decided at this stage are identified and validated by all concerned parties, whereas formalization of final outputs is also enhanced. This process broadly consists of the following steps:

- Build of an initial CGM
- Coordinated regional security assessment in each region (where inter-RSC coordination is already possible)
- Build of revised IGMs/CGM including (preliminary) remedial actions identified in the previous step
- Secondary coordinated regional security assessment
- Final exchange of information between all RSCs and TSOs to consolidate final results of the security analyses and agreement of all decided remedial actions. (A TSO may delegate to its RSC its agreement).

The resulting process is shown in the following scheme.

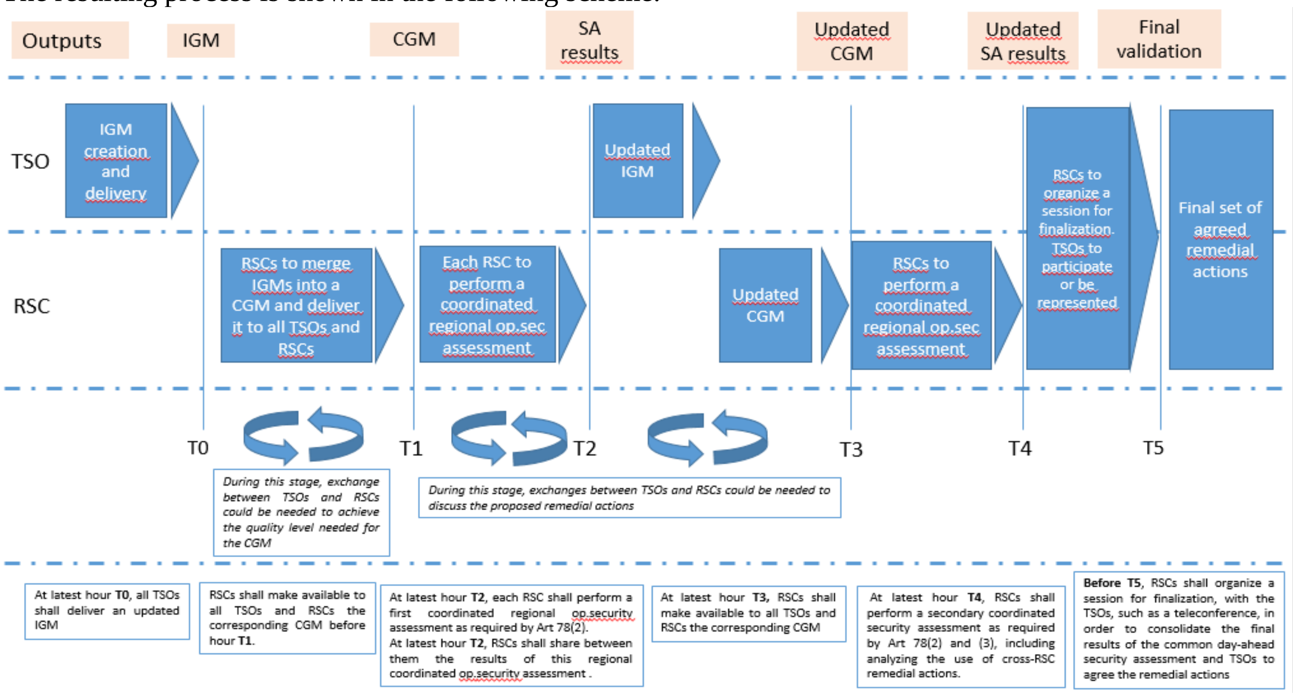


Figure 1

ENTSO-E AISBL • Avenue de Cortenbergh 100 • 1000 Brussels • Belgium • Tel + 32 2 741 09 50 • Fax + 32 2 741 09 51 • info@entsoe.eu • www. entsoe.eu

The result of this process will consist in security assessment results and agreed remedial actions which will be taken as a reference basis. Further intraday security analyses results should be assessed in the intraday with respect to this reference basis.

With respect to the heavily constrained period of the end of day-ahead in the TSOs and RSCs rooms, while ensuring its efficiency, this process needs to start at a given time T0 and end not later than a given time T5. In case there remains some security violations not solved (e.g. no agreement on the remedial actions), Art 33(4) provides that concerned TSOs and RSCs shall agree on the needed steps in intraday to address them at best, and RSCs shall report on these situations in their annual reports.

This process is new and is expected to evolve with practice; it is also expected to evolve in duration because of evolution of tools. For these reasons, and considering this process does not impact other stakeholders, TSOs consider worth not to hard-lock the values of the hours T0 to T5 in the methodology, but to leave them open for definition/update by TSOs, subject to publication on ENTSO-E website. In addition, when the process will have been applied for a maximum of 2 years, all TSOs are required to use the collected experience to review if necessary these Tà to T5 values, notably to assess the opportunities for ending earlier (which could be beneficial for capacity calculation processes and for activation of long-lasting remedial actions) and/or reducing the total duration.

Intraday

In intraday, there is no good argumentation which would justify a request to synchronize the security assessments done by the different TSOs and RSCs everywhere in Europe. It could be even detrimental to the ability to design the most adequate timings, with respect to control area/region specificities. This orientation is also needed to actually leave TSOs of each CCR with their full ability to determine their needs in terms of frequency and hours of coordinated regional security analyses at CCR level in application of SO GL Art. 76-77.

Nevertheless, in order to ensure a minimal common pan-European approach in terms of securing security analyses results with respect to the impacts of uncertainties, which need to update IGM/CGM and assess system security on these updated system forecasts, the CSAM includes a request (Art. 24) for each TSO to run at least 3 coordinated operational security analyses for its control area in intraday. These analyses can be totally or partially covered by the RSC tasks agreed at CCR level. This value is based on a minimum obligation to update security analyses in order to reduce risks of inappropriate decisions made on old inaccurate forecasts and is consistent with the fact that the CGM methodology developed pursuant to SO GL Art. 70 requests all TSOs to update their IGMs at least 3 times in intraday and RSCs to produce corresponding CGMs.

Sequential activities in intraday

In general, in intraday, in order RSCs to realize coordinated regional operational security assessments and TSOs to validate their results, the following tasks have to be performed:

- TSOs have to prepare an IGM with their updated values, included previously agreed remedial actions. When delivering their IGM, they may run local security analyses (called "local preliminary assessment" in CSAM) to identify constraints mainly due to internal flows and include corresponding remedial actions if needed. But those local security analyses are not always pertinent, for example when they are expected to be eliminated when more precise flows are computed on the CGM.

- CGMs have to be built by RSCs
- RSCs have to perform coordinated regional operational security assessment, as requested by SO GL Art 78. This includes reporting to TSOs on congestions identified, proposing needed remedial actions, and exchanging with the TSOs until the remedial actions are agreed (remedial actions may be improved/modified during this step) or refused.
- Where applicable, depending on the agreed capacity calculation methodology in intraday, these steps may be followed by an additional intraday capacity calculation step. Note that such a step is a complex one since capacity calculation processes are long and demanding.

On the other hand, TSOs are requested to run coordinated operational security analyses on their control area, pursuant to SO GL Art 70. In order to clarify the respective scope of these coordinated operational security analyses and the coordinated regional coordinated operational security assessments performed by RSCs, CSAM Article 20 requires TSOs to establish the list of grid elements on which congestions shall be monitored by RSCs. It is worth to note that each TSO may delegate partly or totally its coordinated operational security analyses to the RSC.

It is expected that such a list should comprise all major grid elements whose congestions are influenced by the effects of the meshed interconnected system, but might exclude those grid elements where congestions are due to local flows. Article 20 requires that this list shall include at least critical network elements, since those elements are identified as those mainly affected by cross-border exchanges.

The following scheme represents the successive steps in the day of the different kind of analyses.

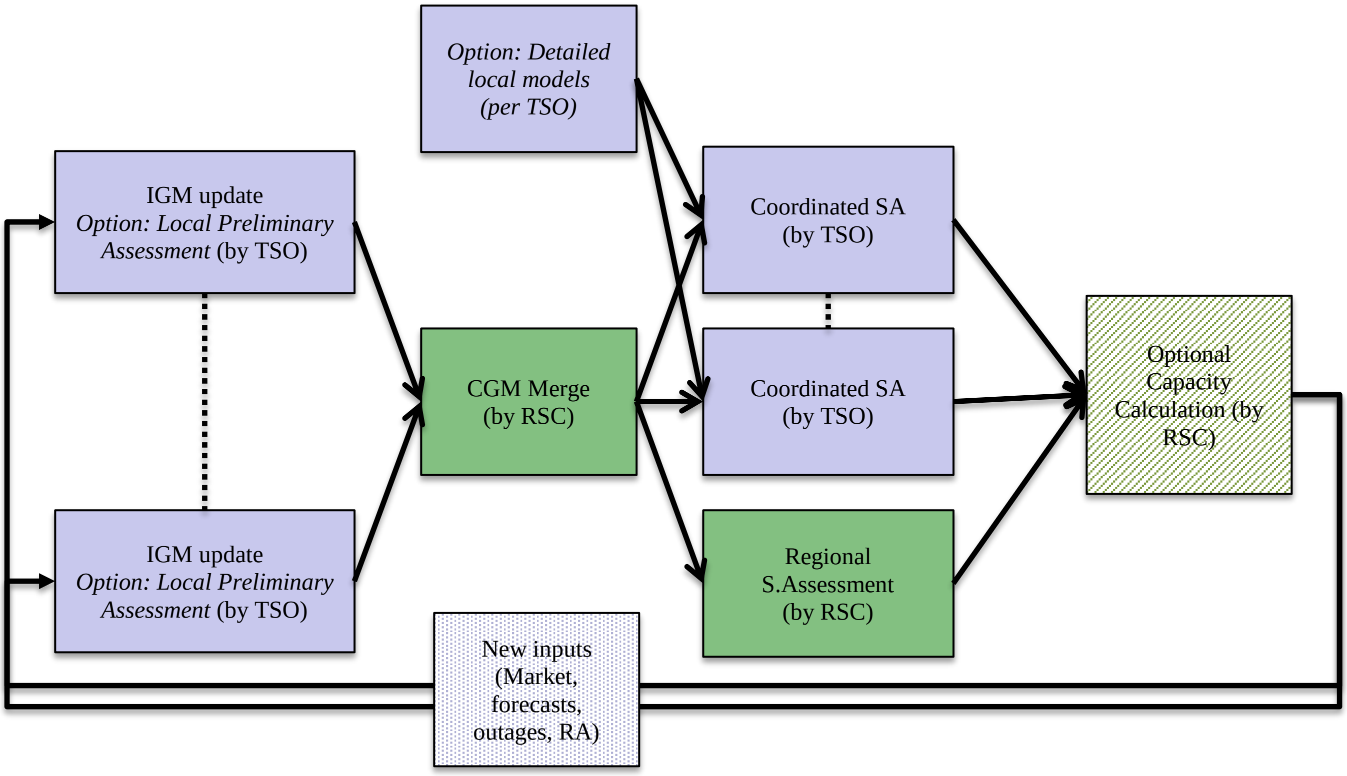


Figure 2

The following table summarizes the respective objectives of the different kinds of security analyses/assessments considered in the methodology.

Type of analysis	References	Objective	Grid model	Run by
Local preliminary assessment	CSAM Article 20	Optional preliminary operational security analysis run to improve the IGM quality, i.e. removing some of the constraints (not likely to be removed by regional coordinated security analysis)	Chosen by TSO when preparing its IGM (e.g. an updated TSO IGM integrated in an "old" CGM)	TSO
Coordinated operational security analysis	SO GL Art 72 (1-4) and Art 74(1)	Each TSO shall ensure security on its control area. It shall share the results with affected TSOs, and prepare remedial actions in a coordinated way when needed Art 77.3 provides that TSOs are supported by the RSC to fulfil this task of performing a coordinated security analysis.	CGM at least (the CGM can be extended/completed e.g. by more local detailed data (low voltage levels)).	TSO It can delegate partly or totally this activity to RSC. It can also perform additional coordinated security analysis
Regional coordinated operational security assessment	SO GL Art 77-78	The RSC shall assess the security of the system at regional level, i.e. on the grid elements that it monitors for TSOs, and proposes remedial actions of cross-border relevance.	CGM	RSC, in interaction with TSOs

3. Influence

3.1 Introduction

Articles 75 and 84 of the SO GL require TSOs to define:

1. methods for assessing the influence of transmission system elements[1] and SGUs located outside of a TSO's control area in order to identify those elements constituting the observability area and the contingency influence thresholds above which contingencies of those elements constitute external contingencies;
2. a methodology for assessing the relevance of assets for outage coordination

Following chapters provide explanations to the Title 2 of the CSAM ("Determination of influencing elements"), and its equivalent in RAOCM.
Firstly, general principles of the method for assessing the influence of external grid elements on a TSO's control area are explained. Furthermore, simple technical reasons for determination of observability area, contingency list and relevant assets list are given.
Then, processes and criteria to be applied by each TSO to identify elements constituting the observability area, the external contingency list and the Relevant Assets list according to Art.75 and Art.84 of the SO GL are described.
At the end, general views on thresholds and their selection are provided.

3.2 Approach for assessing the influence of transmission system elements and SGUs

Introduction

A computation method for assessing the quantitative influence of an external element on a TSO's control area has been identified by all TSOs and is mainly described in Articles 3 and 4 of both methodologies.
Such method is based on the calculation of the so called "*influence factor*" which is, according to the SO GL, the numerical value used to quantify the greatest effect of the outage of a transmission system element located outside of the TSO's control area, excluding interconnectors, in terms of a change in power flows or voltage caused by that outage, on any transmission system element. The higher is the value the greater the effect.
Such "influence factor" can be then compared with an influence threshold (which can vary depending on the scope of the assessment) to decide if the element have a relevant influence or not.
Such a quantitative method is based on the definition of a set of computations to run, including which data model is to be used, how to make computations and finally how to compute the influence factors from these computation results. The description of the computation formulae is provided in the Annex I of the CSAM and RAOCM proposal.

Method for Influence factor determination

[1] Art 75(2) specifies that grid elements located in the network of transmission-connected DSO can be part of the observability area and Art 43(2) of SO GL allows TSOs to consider elements located in the network of non-transmission-connected DSO to be part of the observability area. Therefore, when notion DSO/CDSO is used in this document it is referred to transmission-connected DSO/CDSOs.

The influence of elements located outside TSO's control area being grid elements, generation units and demand facilities on a TSO's control area can be assessed[2] in terms of power flows and/or voltage deviation.
Since voltage regulation are typically a local issue and dynamic aspects are specific in terms of location and nature of the phenomenon to analyse, power flow influence factors are considered the most relevant ones in the scope of the CSAM/RAOCM. In line with this, the CSAM/RAOCM requires that, when a quantitative assessment must be performed, it shall be based on power flow influence factors and, only optionally (according to the TSO who is performing the assessment), on voltage influence factors or dynamic studies. In the case of dynamic studies, this should be organized between involved TSOs and the models and studies used for that determination shall be consistent with those developed in application of Articles 38 or 39 of SO GL.

Influence factors assessment (Figure 3) can be performed in:

a) "Horizontal" direction: when a TSO (e.g. TSO A) is assessing the influence of elements located in another control area (e.g. Control Area B) on its network;
b) "Vertical" direction: when a TSO (e.g. TSO A) is assessing the influence of elements of DSO/CDSOs systems located in its control area.
c) "Diagonal" direction: when a TSO (e.g. TSO A) is assessing the influence of elements located in DSO/CDSOs system directly connected to another TSO (e.g. TSO B)

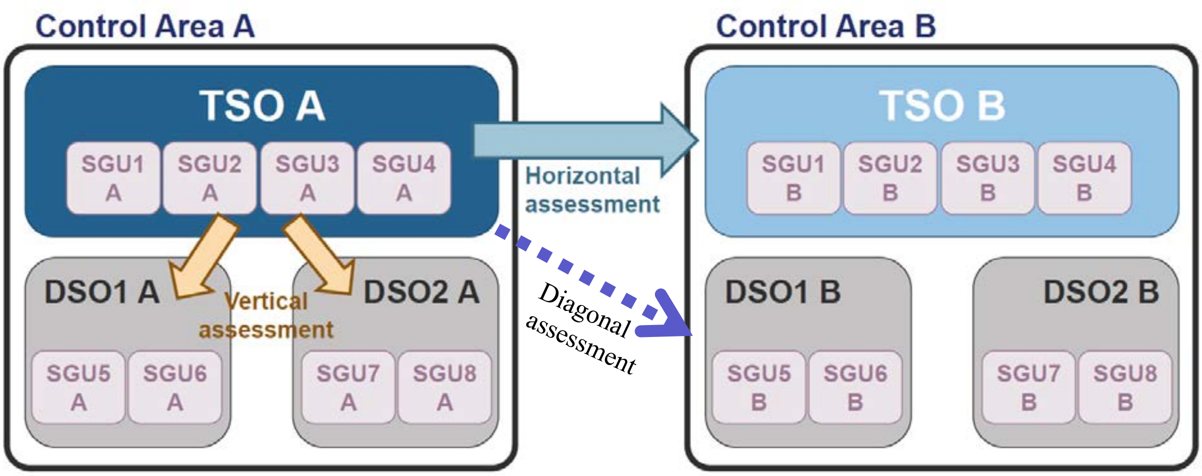


Figure 3

When performing a quantitative "horizontal" assessment, each TSO shall compute influence factors, inside its Synchronous Area (SA), using the Year-ahead scenarios and CGMs developed according to SO GL Article 65, as these scenarios:

- Shall be built every year by TSOs and therefore will be available
- Contain fully meshed grid with normal switching state
- Shall represent different seasonal situations

When performing a quantitative "vertical" assessment, each TSO can compute influence factors using the Year-ahead scenarios and CGMs developed according to SO GL article 67 or its grid model and scenarios considered relevant for the scope of the computations. This grid model has to be complemented with a representation of the parts of the DSO/CDSOs grids which are under assessment, if they are not already available for the TSO.

"Diagonal" assessment can be performed only on the DSO/CDSOs elements that connecting TSO (e.g. TSO B) has modelled in its IGMs developed according to SO GL article 67. In this way it is assumed that the influence of DSO/CDSO elements (e.g. DSO/CDSO B) on connecting TSO (e.g. TSO B) are greater than on other TSOs (e.g. TSO A)."

Year ahead scenarios contain the normal switching state which can be different for different situations. Planned outages are usually not included. To consider different topologies and different thermal capacities of the element, it could be necessary to analyse more than one year ahead scenario (set S of scenarios) during calculation of influence factors.

3.3 Methodology for the Identification of TSO observability area and external contingency list

Introduction

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

Hence, each TSO is due to analyse periodically, by numerical calculations, the external transmission network with influence on its control area. The external contingency list is the result of that analysis and includes all the elements of surrounding areas that have an influence on its control area higher than a certain value, called "*contingency influence threshold*". "*Contingency influence threshold*" means a numerical limit value against which the influence factors are checked and the occurrence of a contingency located outside of the TSO's control area with an influence factor higher than the contingency influence threshold is considered to have a significant impact on the TSO's control area including interconnectors.

Each TSO has to take into account the elements of this external contingency list in its contingency analysis. Therefore, in order to properly assess the security state of the system in its control area and to properly simulate the effect of external contingencies, a TSO has to adopt a model of the external grid wide enough to guarantee accurate estimations (in the control area) when performing the N-1 analysis of the elements of the external contingency list (and of internal list). For this reason, a so called "observability area", larger than the TSO's control area, must be identified and monitored. Such an observability area is also necessary to perform correct estimation of the real-time values on the elements belonging to the control area.

"*Observability area*" means a TSO's own transmission system and the relevant parts of distribution systems and neighbouring TSOs' transmission systems, on which the TSO implements real-time monitoring and modelling to maintain operational security in its control area including interconnectors

All the external elements with an influence on the control area higher than a certain value, called "*observability influence threshold*" (equal or lower than the "*contingency influence threshold*"), constitute the "*observability list*". The "*observability list*" could be a non-consistent model. For example, a certain external line could be part of the observability list meanwhile its neighbour branches are not in this list. Therefore, the model must be completed with additional network elements and some equivalents to obtain the consistent and fully connected observability area. The observability area includes the control area and the external network, so each TSO is able to simulate properly any contingency of the internal and external contingency list when performing the N-1 analysis (Figure 4).

The observability area represents the minimum set of grid elements for which a TSO is entitled to receive data (electrical parameters, real time measurements) from the owner or the entity in charge of them.

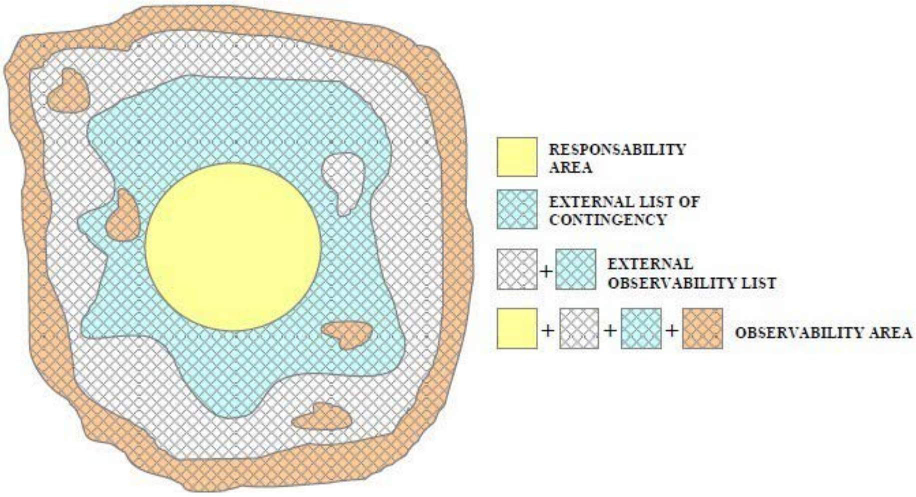


Figure 4

The definition of an external contingency list and an observability area is mainly needed for the application of SO GL requirements for the close to real time operational security analysis, because for security analyses ahead, the following requirements apply:

- For security analyses up to and including intraday analyses, Art. 72(4) requires that a TSO shall use "at least the common grid models established in accordant to Articles 67 to 70";
- For security analyses up to and including intraday and close to real-time analyses, Art. 77(3)(a) prescribes that each TSO shall use the results of tasks delegated to a regional security coordinator. Art. 78(1)(a) prescribes that each TSO shall provide the regional security coordinator with its updated contingency list and Art. 78(2)(a) prescribes that the regional security coordinator shall perform regional security assessments on the basis of a common grid model and of the contingency lists provided by each TSO. These requirements ensure that the regional security coordinator will perform the security analyses on a common grid model (larger than any observability area) and taking into account all the contingencies mentioned by each TSO of the capacity calculation region.

Nevertheless, individual grid models are in general derived from initial real-time snapshots. As such, an appropriate quality of the observability area is a prerequisite to establish good quality snapshots and IGMs and, consequently, establish trustable CGMs.

Process for Observability Area identification

With ever growing decentralized production from renewable energy sources, influence of DSO/CDSOs elements on the transmission system increases. To have better state estimations and improve security assessment, TSOs could have the need to expand their observability area in vertical direction i.e. to the DSO/CDSOs grids.
The process set up in the Article 5 of CSAM for identifying external elements to be included in a TSO's Observability Area is based on 3 main steps (Figure 5):

a) <u>Qualitative vertical assessment:</u>

The TSO in coordination with DSO/CDSOs can identify in qualitative way DSO/CDSOs elements which inclusion in observability area list may be necessary. If the TSO and DSO/CDSOs agree on this approach and on the effective list of elements which shall be part of TSO's observability area, then the TSO shall not be obliged to do the assessment for these elements and will not require the data model from DSO/CDSOs to proceed to this assessment.

b) <u>Quantitative vertical assessment:</u>

If an agreement in step 1 cannot be found, TSO shall use the mathematical method provided in the Annex I of CSAM for assessing the influence of elements.

To perform such calculation TSOs have to use sufficiently detailed grid models in order to have results. For this reason, each TSO shall ask DSO/CDSOs for technical parameters and data which may be necessary for creating such a model. For vertical assessment TSO can use either its grid model or CGMs developed according the Article 67 of SO GL; these models shall be complemented with data provided by DSO/CDSOs. The request to DSOs/CDSOs to provide such data should be limited to what is necessary to process the computations and identify the parts of their grids which are captured by the assessment method, hence avoiding DSOs/CDOS to have to provide huge descriptions of their total grids.

If a DSO/CDSO element has an influence factor higher than the *observability influence threshold*, it will be included in corresponding TSOs lists (with additional elements needed to obtain fully connected observability area). For these elements DSO/CDSOs shall provide structural and real-time data to the TSO according to SO GL requirements.

c) <u>Quantitative horizontal and diagonal assessment:</u>

TSO shall use the mathematical method provided in the Annex I of CSAM for assessing influence of elements located in other Control Areas. If such element has an influence factor higher than the *observability influence threshold,* it will be included in corresponding TSOs lists (with additional elements needed to obtain fully connected observability area).

If during this assessment TSO detects a DSO/CDSO element located outside its control area, assuming that DSO/CDSO grid is modelled, to be included in its corresponding list, technical parameters, structural, forecast and real-time data of DSO/CDSO elements and additional elements needed to obtain fully connected observability area have to be exchanged between TSOs.

TSOs may also use dynamic studies (e.g. rotor angle evaluation, but not limited to it) for assessing the influence of elements located outside its control area or in DSO/CDSO directly connected to it, using models, studies and criteria, consistent with those developed in application of Articles 38 or 39 of SO GL.

Technically TSO's observability area will consist of elements, identified as described in previous steps, and all the busbars to which these elements could be connected. To have accurate state estimations and to be able to assess its system state by preforming contingency analysis (N-1 analysis) TSOs must have all injections and withdrawals on these busbars. For these reasons, each impacted TSOs and DSO/CDSO shall provide real time data related to these busbars to the concerned TSO according to Articles 42.(2) and 44 of SO GL. In some cases (e.g. SGUs connected to DSO networks), TSOs can choose to represent these SGUs in an aggregated manner.

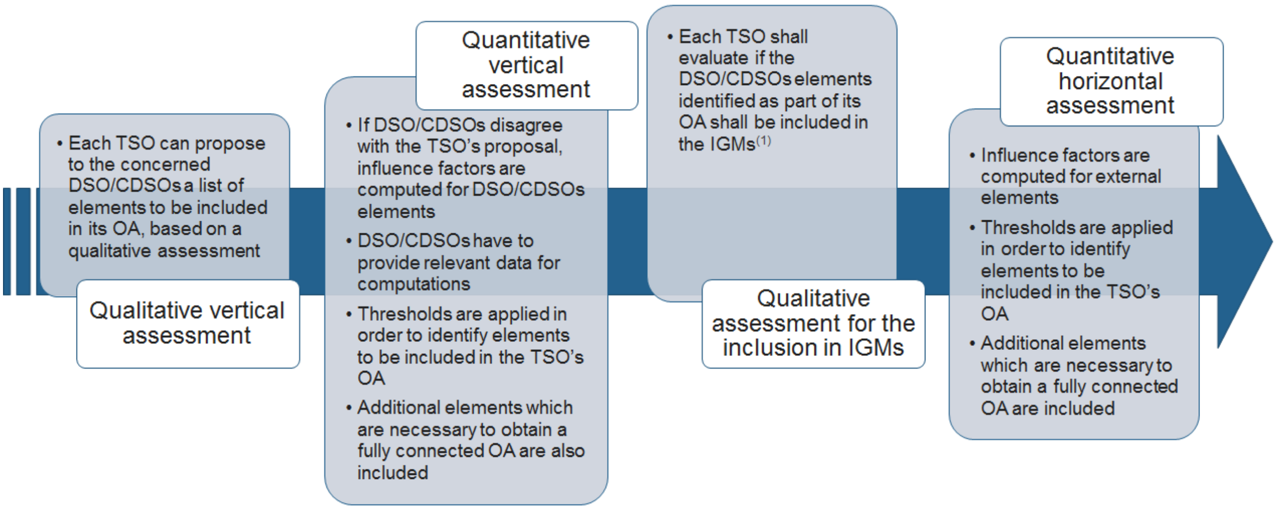


Figure 5

Process for Contingency List identification

As required by Article 33 of SO GL each TSO shall define a contingency list, including internal and external contingencies of its observability area. Article 6 of the CSAM provides the steps for identifying the minimum set of external elements, which shall be included in a TSO's (external) contingency list (Figure 6):

a) <u>Qualitative vertical assessment:</u>

If in the process of observability area identification the TSO and the DSO/CDSOs agree on the effective list of elements which shall be part of the TSO's observability area based on a qualitative assessment, the elements to be part of the TSO's external contingency list may be identified based on a qualitative assessment.

TSOs external contingency list may be complemented with any of the generating modules and demand facilities connected to a busbar being part of the TSO's observability area. Since there is not a direct impact on SGUs included in the contingency list, TSOs can determine such a need on a qualitative basis and are not required to perform computations for the inclusion of a SGU's asset in the contingency list.

b) Quantitative vertical assessment

If TSO's observability area in vertical direction was defined using quantitative vertical assessment, identification of DSO/CDSOs elements, which will be part of TSOs contingency list, will be done using mathematical method provided in the Annex I of CSAM.

If a DSO/CDSO element (included in the TSO's Observability Area according to paragraph 3.2) has an influence factor higher than the *contingency influence threshold*, it will be included in corresponding TSOs contingency list.

c) Quantitative horizontal and diagonal assessment:

TSO shall use the mathematical method provided in the Annex I of CSAM for assessing influence of elements located in other control areas. If an element located outside the TSO's control area has an influence factor higher than the *contingency influence threshold*, it will be included in corresponding TSOs contingency list.

d) Qualitative horizontal assessment:

External contingency list may be complemented with any of the generating modules and demand facilities connected to a busbar being part of the TSO's observability area.

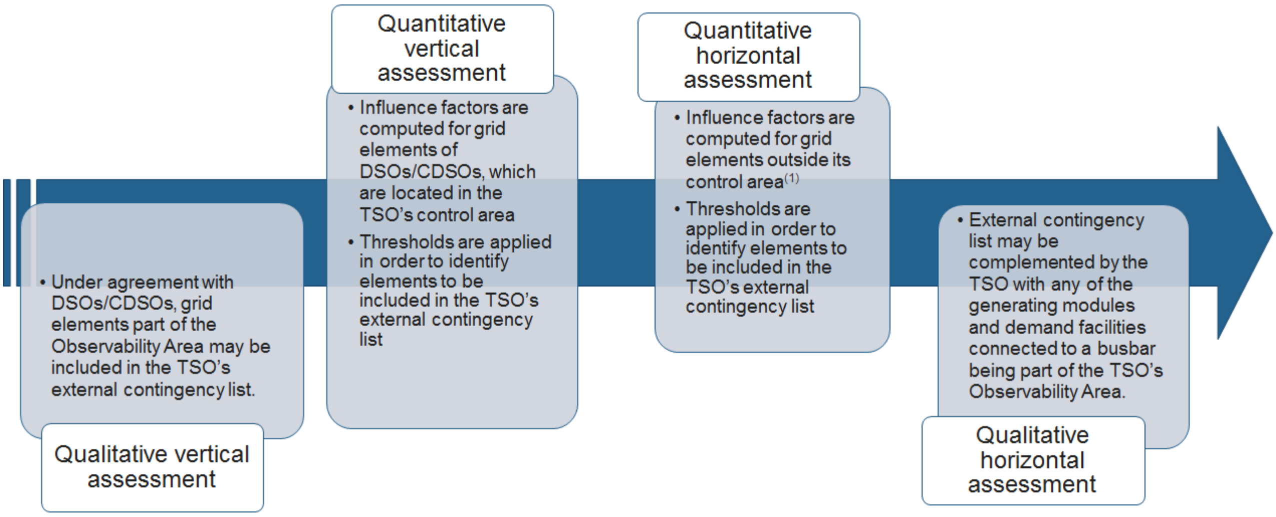


Figure 6

Update of TSO observability area and external contingency list

Main goal of the methodology described above is to have harmonized quantitative approach for defining observability and external contingency lists at synchronous area level. For this reason, a first harmonized assessment (based on this approach) shall be performed once the CSAM is approved.

Then, taking into account that significant changes in the influence factors can be induced only by (relevant) changes in the grid structure, it is not needed to impose a frequent update of the mathematical assessment, which requires time and resources to be performed.

For this reason, a 5 years period is considered the optimal compromise between the necessity to monitor the evolution in the influence factor and the necessity to not spend resources for unnecessary assessments. This does not prohibit TSOs to do assessment more frequently.

3.4 Methodology for assessing the relevance of generating modules, demand facilities, and grid elements for outage coordination (Art. 84) - RAOCM

Introduction

A definition of "relevant assets" has been introduced in the SO GL to ensure that only those elements participate in the outage coordination process whose individual availability statuses have a significant influence on another control area (e.g. larger Power Generating modules that are closer to the border are more likely to be qualified as relevant assets than smaller units that are farther from the border). Hence relevant assets are defined as those assets, whether they are grid elements, power generating modules or demand facilities, for which the individual availability status has an impact on the operational security of the interconnected system.

In order to assess the relevance of a given asset, TSOs jointly developed an approach that is aligned to the one adopted for identifying observability areas and external contingency lists.

Process for Relevant Asset List identification

ENTSO-E AISBL • Avenue de Cortenbergh 100 • 1000 Brussels • Belgium • Tel + 32 2 741 09 50 • Fax + 32 2 741 09 51 • info@entsoe.eu • www. entsoe.eu

Article 5 of RAOCM provides steps for identification of elements which could be relevant for outage coordination process. Furthermore, RAOCM provides TSOs of each CCR with a process allowing the determination of the relevant assets list and defines requirements concerning updates of relevant assets list.

Once power flow influence factors (and, where relevant, voltage influence factors) of grid elements, generating modules and demand facilities located outside TSO´s control area have been computed according to the mathematical method published by all TSOs they can be compared with an appropriate relevance influence threshold, for determining the relevant asset list proposals. If the influence factor of an external element is higher than the threshold, this element should be considered as part of the relevant asset list proposal of the TSO. Such thresholds can be different for power flow influence factors and voltage influence factors.

Relevant asset list proposal shall be also complemented with:

- all grid elements located in a transmission system or in a distribution system which connect different control areas (as required in SO GL);
- all combinations of more than one grid elements whose simultaneous outage state can be necessary for any particular material or system reason and which can threat the system security, according to TSO's experiences. This is needed because, in the described approach, no contemporaneity of outages (i) is considered;
- all elements which outage status can have an impact on the operation (such as reducing physical capacity) of DC links between SAs;
- critical network elements identified in accordance with Regulation (EU) No 2015/1222 for the relevant outage coordination region[3], provided that their status of critical network element is stable throughout the year. The list of critical network elements is defined differently for each capacity calculation region and can change over time.

Since a methodology aimed at identifying relevant assets at synchronous area level should be simple enough (based on one outage) to be implementable and to produce results in a proper time, not all the possible combinations of outages can be tested. For this reason, each TSO shall include in its relevant assets list proposal combination of outages which based on experience could significantly affect the neighbouring control areas.

All TSOs of each CCR shall define the relevant assets list based on TSOs proposals and according the process defined in Article 5 of RAOCM.

Influence factor of SGUs

Power flow influence factors for generating modules and demand facilities should be assessed using the same formulas adopted for grid elements (provided in the Annex I of RAOCM), considering them as the r element. Contrary to grid elements, the outage of a generating module or a demand facility leads to an imbalance between generation and demand. The impact on the balance between generation and load of a planned outage of a generating module/demand facility is different from the impact of a contingency. In the first case, the market rules will provide for a balance equilibrium, the unavailable generation being compensated by local other units or by imports. In the second case, the balance will be ensured by reserve activation. These differences can result in different impacts

[3] The Outage Coordination Region shall be considered equal to the Capacity Calculation Region unless all concerned TSOs agree to merge two or more outage coordination regions into one unique outage coordination region.

on the security of the grid between the planned outage and the tripping of the same element. As a result, influence factors for assessing the relevance of generating modules and demand facilities for outage coordination should be computed restoring the net balance of the control area or the control block in which the generator/demand facility is located when computing P^{t}_{n-i-r}. Such restoration should be performed according with a pro-rata approach on the dispatchable generators already activated in the TSO's control area or control block.

Update of the Relevant Asset List

The harmonization of the approach to be adopted for defining the relevant asset list of each outage coordination region is the main goal to be achieved applying the methodology described above, especially trough the quantitative assessment of the influence factors. For this reason, a first harmonized assessment (based on this approach) shall be performed once the methodology is approved. Then, taking into account that significant changes in the influence factors can be induced only by (relevant) changes in the grid structure, it is not needed to impose a frequent update of the mathematical assessment, which requires time and resources to be performed.

For this reason, if no major changes are observed in the grid structure (e.g. commissioning or decommissioning of assets that can affect influence factors of already existing elements) a 5 years period is considered the optimal compromise between the necessity to monitor the evolution in the influence factor and the necessity to not spend resources for unnecessary assessments. Additionally, a more stable list of the relevant assets is seen as an added value for the stakeholders: for example, the decision to invest in IT system for facilitating the information exchange required in the SO GL can be taken in an easier way if they already know that, once included, they will be in the list for a long period.

Relevance of elements commissioned between two mandatory relevance factors computations, can be performed in qualitative way. If the owner of the new element disagrees with such approach, TSO shall use method for assessing influence of elements defined in previous chapters.

Anyhow, taking into account the requirement set in Article 86.1 and Article 88.1 of SO GL, a yearly qualitative re-assessment of the relevant asset list shall be performed in order to better monitor the quality of such list.

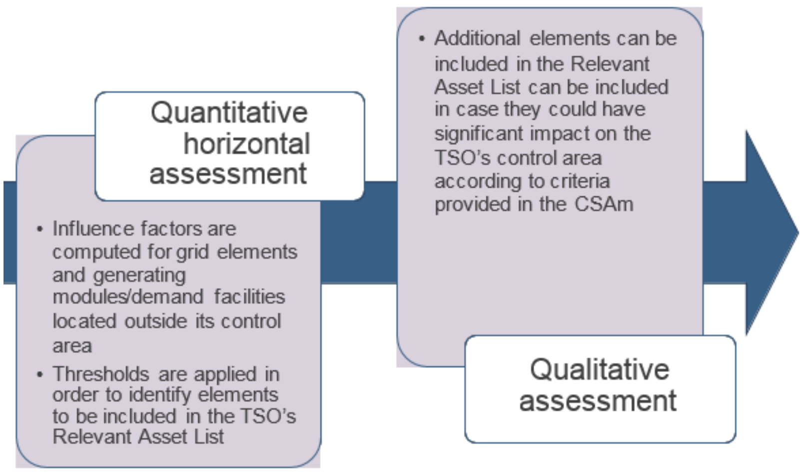


Figure 7

ENTSO-E AISBL • Avenue de Cortenbergh 100 • 1000 Brussels • Belgium • Tel + 32 2 741 09 50 • Fax + 32 2 741 09 51 • info@entsoe.eu • www. entsoe.eu

3.5 Influence thresholds selection

According to the CSAM, RAOCM and the processes described in chapter 3 of this document, when a quantitative assessment is applied, thresholds have to be defined for performing proper selections. 3 different thresholds have been identified:

- *observability influence threshold*
- *contingency influence threshold*
- *relevance influence threshold*

Defining a common threshold for each list at the level of Synchronous Area is not achievable and not advisable:

- Some TSOs need a larger view on the rest of the interconnected system due to the structure of their grid and the conditions under which they operate their grid (typically loading and margins, cross-border market activity and loop flows, actions of other TSOs, etc.)
- For other TSOs this necessity is lower and it is not efficient to impose them to invest more resources on it. It would be detrimental to the application of SO GL Article 4(2)(c) to impose the same threshold to these TSOs than the one needed for the previous ones.

Hence, the CSAM and RAOCM set rather small individual ranges for each of the lists. For each list, each TSO shall select and publish a unique value from the respective ranges for each threshold. The threshold values shall be identical regardless of the grid element – or where applicable generation module or demand facility – of which the influence is assessed by the TSO.
The ranges have been defined taking into account some general principles as well as expert's knowledge and comparison with previous practices. Examples for general principles taken into account are:

(1) Thresholds shall not be lower than the expected precision of measurements in a SCADA, including state estimation improvement. Such a precision can be estimated roughly around 1 – 3 %.

(2) Thresholds shall not be higher than those needed to identify a change in a flow, deemed as relevant on the basis of operators' experience. For example, a change of more than 10 to 25 % in the flow[4] (due to any reason) is seen as warning information needing careful evaluation and monitoring from a dispatcher.

(3) Thresholds for observability area definition should be lower than for external contingency list definition, because the observability area is at the basis of the quality of the computations and because external contingency items are a subset of items constituting the observability area.

(4) Thresholds shall not be too high since only the impact of single outages are considered in the mathematical approach while, in real-time operation, the contemporaneity of different outages can appear.

Besides such general principles, the influence computation method was tested using reference data sets of the Continental Europe Synchronous Area for winter 2016/2017 and summer 2017. Based

[4] e.g. 200MW of change on a "big" line in 400 kV, with a N flow in the vicinity of 2000 MW

ENTSO-E AISBL • Avenue de Cortenbergh 100 • 1000 Brussels • Belgium • Tel + 32 2 741 09 50 • Fax + 32 2 741 09 51 • info@entsoe.eu • www. entsoe.eu

on the computation results, lists of elements resulting from different thresholds were generated. These were evaluated by experts of several TSOs to determine which thresholds lead to technically sensible results. These evaluations included comparisons with lists resulting from proven practices previously used in order to take into account the corresponding know-how. Based on the feedback of the TSOs experts, the different ranges of thresholds were narrowed down as much as possible.

Observability influence threshold

The choice of the observability power flow influence threshold (and, where relevant, of the observability voltage influence threshold) by each TSO should have the following properties:

- low enough to guarantee good quality results of real-time state estimation and operational security analysis;
- high enough to avoid too big observability areas (which can induce higher costs and excessive time requirements for online computations).

Contingency influence threshold

The choice of the contingency power flow influence threshold (and, where relevant, of the contingency voltage influence threshold) by each TSO should have the following properties:

- low enough to minimize the risk that the occurrence of a contingency identified in another TSO's control area and not in the TSO's external contingency list could lead to a TSO's system behaviour deemed not acceptable for any element of its internal contingency list; the occurrence of such a contingency shall notably not lead to an emergency state;
- high enough to avoid too long contingencies lists that are not compatible with time requirements for operational security analysis.

Relevance influence threshold

The choice of the relevance power flow influence threshold (and, where relevant, of the relevance voltage influence threshold) by each TSO should have the following properties:

- low enough to minimize the risk that outages of not relevant grid element could treat the security of neighbouring control areas;
- high enough to avoid too long relevant asset lists that would be not necessary, thus leading to an inefficient process, potentially not compatible with time requirements of the outage coordination process.

ENTSO-E AISBL • Avenue de Cortenbergh 100 • 1000 Brussels • Belgium • Tel + 32 2 741 09 50 • Fax + 32 2 741 09 51 • info@entsoe.eu • www. entsoe.eu

3.6 Power flow Identification influence factors and Power Flow Filtering factors: how they are complementary

The Power Flow Filtering influence factor on flows is the maximum Outage Transfer Distribution Factor[5] of an external element r on any given internal element t in any scenario and taking into account any element i disconnected.

Hence, $IF_r^{pf,f}$ expresses the increase of flow on branch t after tripping of branch r in relation to the flow on branch r in n condition (when the element i is out of service), as shown below.

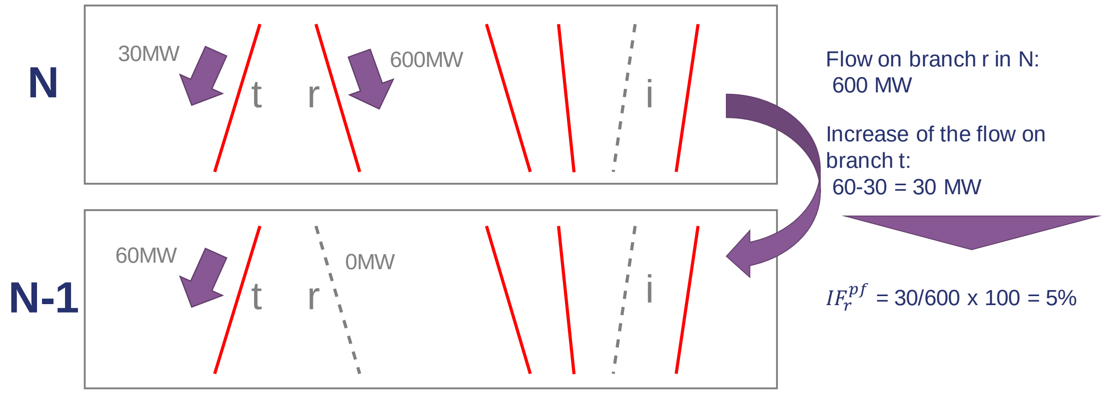


Figure 8

When computing the Power Flow Identification influence factor, the Outage Transfer Distribution Factor (OTDF) is multiplied by the ratio of Permanent Admissible Transmission Loading between the influencing element r and the influenced element t.

The Power Flow Filtering influence factor is only an image of the load transfer and is independent on the flow of the assessed element. The Power Flow Identification influence factor assesses the influence of an external element r on the internal element t taking into account the PATL of the elements involved.

As a consequence, it emphasizes the consequences of a load transfer from a high capacity element on a low capacity element. This approach aims at guaranteeing that the outage of a highly loaded element does not endanger elements with a low capacity. Since influence on flows is assessed independently on the loading of the element in the investigated scenarios, using elements PATL allows simulating the consequences of highly loaded elements outages. Thus, for external contingency lists, the Power Flow Identification IF is more relevant than the Power Flow Filtering IF as it is much more significant for system security, better describing the risk of overload.

Anyhow, using this approach, low PATL external elements may be excluded even if they have a high Power Flow Filtering influence factor. It could be problematic in the determination of the observability area. However, results showed that normalized approach shall be also preferred when assessing the observability area. Indeed, without normalization, many small elements located in lower voltage levels have a high influence factor. Using a non-normalized approach could lead to

[5] *Outage Transfer Distribution Factors (OTDFs) are a sensitivity measure of how a change in a line's status affects the flows on other lines in the system*

ENTSO-E AISBL • Avenue de Cortenbergh 100 • 1000 Brussels • Belgium • Tel + 32 2 741 09 50 • Fax + 32 2 741 09 51 • info@entsoe.eu • www. entsoe.eu

an important increase of elements of the observability area, although these elements are not needed to describe it correctly.

The selection with a normalized approach gives results more in line with the current description of the current observability areas in Continental Europe, highlighting the regional 400kV frame.

However, computation of the Power Flow Identification influence factors requires the introduction of a ratio of PATLs which can be rather high. In some cases, a high Power Flow Identification influence factor may be the result of a combination of a high PATL ratio and of an OTDF so small that it is of the same order of magnitude as the expected precision of measurements in a SCADA. Such cases must be discarded from the results by filtering elements or SGUs whose Power Flow Filtering influence factor on flows is lower than a threshold representative of the expected precision of measurements in a SCADA.

Hence: an element shall be included in a set if its Power Flow Identification influence factor on flows is higher than the "Power Flow Identification threshold" provided in the CSAM or RAOCM and if its Power Flow Filtering influence factor on flows is higher than the "Power Flow Filtering threshold" provided in the CSAM or RAOCM.

In the way it is computed, influence of an element on flows is independent on the load/generation pattern (as an approximation in AC approach, strictly in DC approach) which allows assessing the influence of elements on a limited number of scenarios. Annex II of this document provides more information about why the generation pattern and level of flows in the respective scenarios have a negligible effect on the influence factors calculated in accordance with CSAM and RAOCM.

4. Risk Management

4.1 Introduction

Coordinated operational security analyses deal with the identification of risks on the interconnected system of operational security limits violations, trying to find the appropriate remedial actions, according to SO GL Article 21, and ensuring the coordination of these remedial actions.
In order to ensure system security, TSOs have to assess the consequences of events that are unscheduled but likely to occur on the system, and ensure that the grid remains secure after the occurrence of any of those events taking into account the identified remedial actions. When identifying the most effective and economically efficient remedial actions, TSOs have to make sure that the application of these remedial actions does not endanger neighbouring TSOs grid by coordinating them. This chapter covers thus the parts of SO GL Article 75 referring to principles for common risk assessment.

4.2 Risk Management principles

In current practices, not only in Europe but also in most large grids among the world, risk management is handled through the N-1 principle meaning that the grid operations must remain secure after the loss of any single element of the grid. This security is strengthened by the application of the N-k principle according to which the simultaneous loss of several elements that is likely and stressful enough to be taken into account does not endanger the operation of the system.
This process is performed in three consecutive steps:

- Identification of events to be covered
- Assessment of their consequences
- Identification of necessary remedial actions

SO GL provide rules on how to perform those three steps. This methodology develops them by providing harmonisation for the following principles:

- Definition of the type of contingency that will be monitored and the system secured against, covered by articles 7 to 11;
- Definition of acceptable consequences in term of material limits or energy not supplied, covered by articles 12 to 13;
- Application and when needed coordination of remedial actions, covered by articles 14 to 21.

The overall process can be summarized as follows:
"In addition to the Ordinary Contingencies, each TSO shall define Exceptional Contingencies fulfilling either a set of criteria based on occurrence increasing factors expressing an increase of the probability of such event or having an impact deemed unacceptable and for which the contingencies will have to be covered and will be part of the contingency list.
Each TSO will assess the impact of all events of the contingency list based on simulation.
For each contingency in the Contingency list, each TSO shall accept no violations of the Operational Security Limits or, in case of violation of Operational Security Limits, the result of the loss of the concerned grid elements shall

- *Not lead to violations of the Operational Security limits outside the Control area of the concerned TSO or outside any extension of this control area resulting from multilateral agreement with neighbouring TSOs on "Controlled area accepted consequences"; and*
- *Respect the national obligations in term of acceptable local consequences*

When necessary, each TSO will have to prepare and activate in due time preventive and/or curative remedial actions in coordination with other TSOs when required, with the support of RSCs where this is applicable."

These principles are illustrated by the diagram shown in Figure 9. Each step of this process will be further discussed in the following sub-chapters.

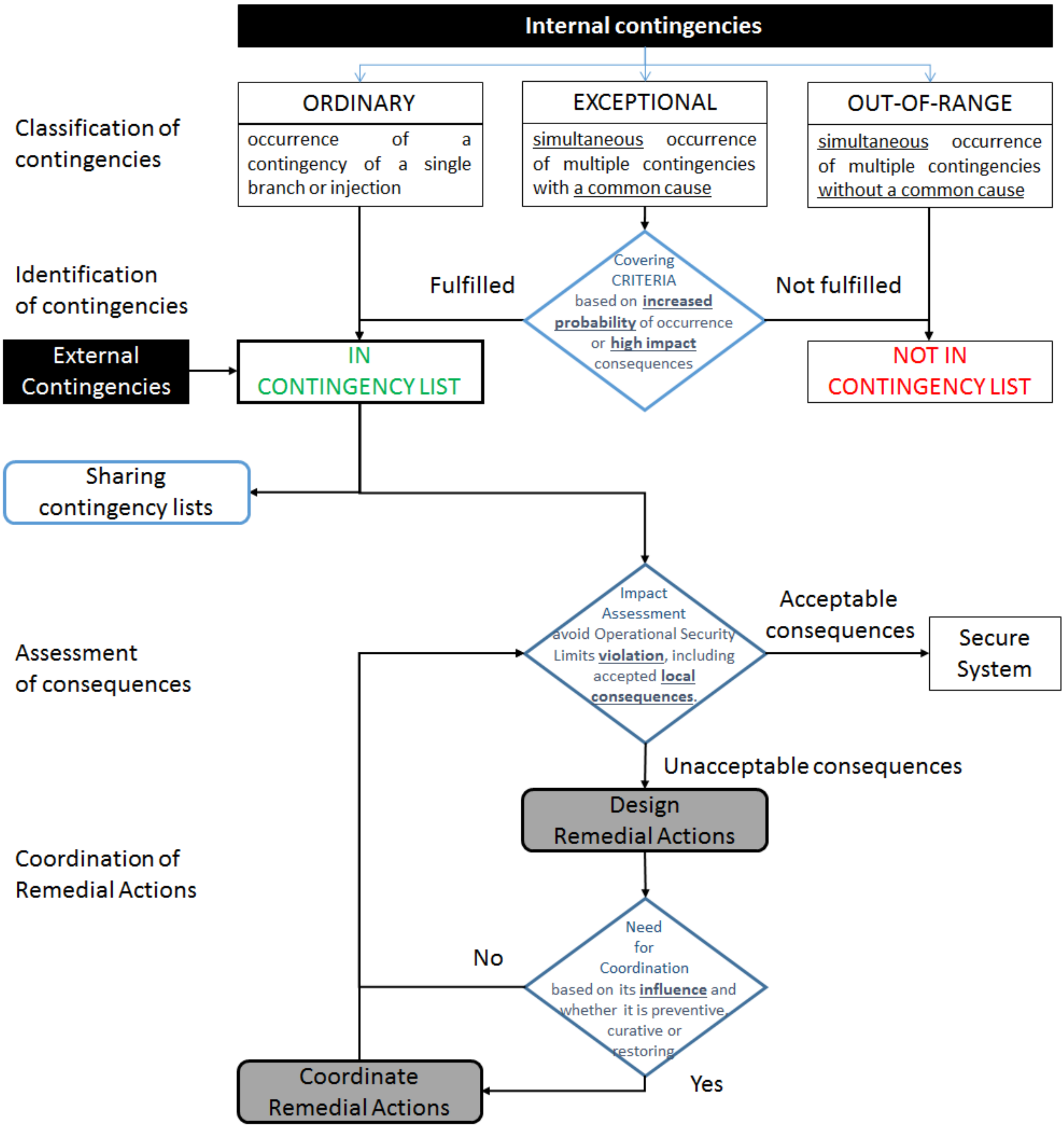


Figure 9

4.3 Assessment of consequences

Consequences of the occurrence of a contingency on the electrical system, and as a result the consequences criteria are examined in this chapter regarding the following dimensions:

1. Material and operating limits;
2. Extent of consequences (local or not);
3. Consequences on grid users (Energy Not Supplied, Power cut).

Activation of remedial action ex-ante versus ex-post the occurrence of a contingency and coordination of such remedial action when relevant are discussed in chapter 4.5.

Material and Operating Limits

Operational security limits are defined by TSOs to protect the people at the vicinity of the materials (near conductors), to protect the material integrity by respecting their technical limits or to respect contract commitments.

According to Article 25 of SO GLs, operational security limits are specified by TSOs for each element of their transmission system taking into account voltage limits, short-circuit current limits and current limits in terms of thermal rating including the transitory admissible overloads where allowed.

According to Article 35 of SO GLs, each TSO has to respect the N-1 criterion, meaning that no violation of operational security limit of any element shall occur following any contingency of his contingency list. TSOs may derogate to the N-1 criterion if the consequences do not propagate to the whole interconnected system.

Evolving contingency

After the occurrence of a contingency, the application of remedial actions may not suffice to solve every operational security limits violation. For safety reasons, grid elements or users in violation of their operational security limits have to be considered as disconnected also. This disconnection phenomenon may result from protection activation or action by an operator. Such events are called evolving contingencies and are said to be verifiable if each and every step can be simulated until a stable state is reached. Obviously, as SO GL Article 35(1) requires TSOs to assess that operational security limits are respected in the (N-1) situation, an evolving contingency which is not verifiable is unacceptable.

To assess that a contingency is a verifiable evolving contingency, a TSO may for example perform the following iterative process:

- Perform a computer based simulation of the contingency
- If operational security limits are violated apply remedial actions
- If those remedial actions are not sufficient or are deemed not efficient, simulate the tripping of the elements or users whose operational security limits.
- Repeat from point 2 until a stable state is reached.

If no stable state is reached or if the (N-1) situation can no longer be simulated, the contingency is not deemed a verifiable evolving contingency.

Figure 10 shows an example of evolving contingency in which a contingency of line A leads to overloads on line B and C. With remedial actions (topology for an example) applied either in preventive or curative way, the overload on line B is solved but not the one on line C. The tripping of line C leads to a power loss limited to the grey area.

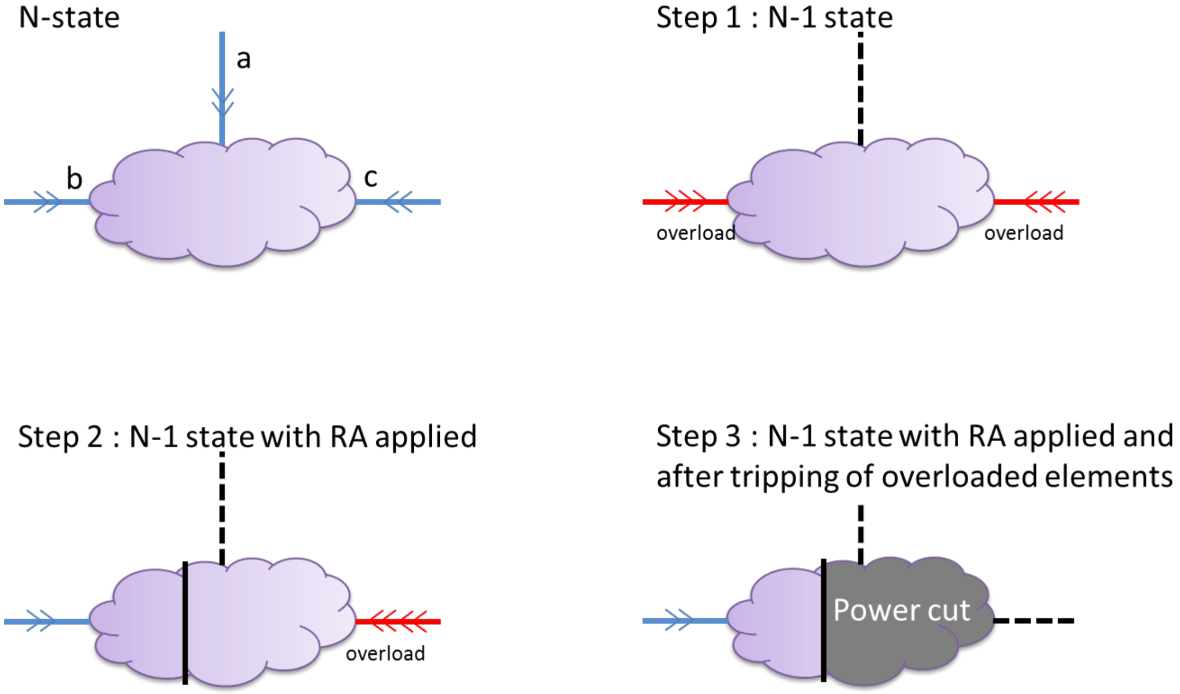


Figure 10

Impact Analysis & Acceptable consequences

CSAM Provides in article 13 that the consequences of a contingency occurring in a TSO's control area are acceptable as long as they are regarded as local, meaning that they do not impact the Operational Security of the interconnected transmission system. This local extension means that they may be either restricted to the TSO's control area where the operational security limit violation appears or spread over one or more other TSO's control area. In the latter case, affected TSOs must jointly agree on this possibility of extension.

As a conservative approach, which is the basis of SO GL, the system is considered secure as long as no contingency for the contingency list leads to operational limits violation. This may not be the most technically and economically efficient way to handle some particular contingencies as a little chance of power cut may be preferred to a costly certain remedial action activation.

For this reason, CSAM introduces in article 12 the possibility that TSOs may, in the respect of their national legislation or internal rules, accept operational limits violation provided that the evolving contingency is verifiable. This means that the consequences of the tripping of the elements violating their operational limits are restricted to a known perimeter, and if all affected TSOs agree on it.

In addition, as frequency is not identified by SO GL Article 25 as a physical characteristic on which TSOs have to define operational security limits since they are defined at synchronous area level, CSAM makes explicit that the consequences of a contingency monitored by TSOs must not result in a power deviation between generation and demand higher than the reference incident.

4.4 Identification of contingencies

Classification of Contingencies

A "contingency" means the possible or real loss of any element of the transmission system, grid element or a significant grid user, or possible or real loss of any element of the distribution system which is relevant for the transmission system's operational security. This loss cannot be predicted in advance (in that sense, a scheduled outage is not a contingency).

SO GLs define 3 types of contingencies:

- Ordinary contingency means the occurrence of a contingency of a single branch or injection;
- Exceptional contingency means the simultaneous occurrence of multiple contingencies with a common single cause;
- Out-of-range contingency means the simultaneous occurrence of multiple contingencies without a common cause, or a loss of power generating modules with a total lost capacity exceeding the reference incident.

Based on those definitions, CSAM Article 7 provides the following harmonized classification of contingencies as shown in Figure 11.

Figure 11

Any other type of contingency resulting from the simultaneous loss of one or several grid users/elements not listed above shall be classified in one of the three categories (ordinary, exceptional or out-of-range) according to the SO GLs’ definitions.

Contingencies probability

Through their definitions, there is no explicit link between these types and their probability of occurrence. However, this probability level is an underlying element which has been taken into consideration when these types have been defined. In that sense,

1. Ordinary contingencies have a rather high probability so that they will always have to be monitored and covered, independently from any occurrence increasing factors;
2. Exceptional contingencies have a probability depending on the specific factors that may increase the occurrence of a “common cause” so that these contingencies will be considered according to the presence or absence of these occurrence increasing factors and/or, independently of their probability, because of consequences high enough to balance the cost of necessary remedial actions;
3. Out-of-range contingencies have such a low probability that they will never be monitored or covered, even considering the impact of occurrence increasing factors.

According to the SO GLs, Exceptional Contingencies consist of multiple contingencies with common cause. The common cause refers to a structural dependency of the contingencies which makes the probability of simultaneous occurrence of these contingencies highly dependent on occurrence increasing factors such as permanent or temporary conditions like the environment, the inherent performance of the equipment, maintenance assessment,…These occurrence increasing factors can have a big or a small occurrence increasing on the probability, so that if some of them marginally alter this probability, other factors have a significant effect on this probability. "Significant" means that they lead to such an increase of the probability of occurrence that it shall change the way the concerned multiple contingency will be managed during the risk assessment. Two types of occurrence increasing factors are introduced whether they are time dependent (temporary) or not (permanent) and some examples are provided below.

1. Permanent occurrence increasing factors:
    a. Specific geographical location[6], as examples
        i. Lines built in mountains where the profile of the landscape and instability of the ground may increase risk of tower incident;
        ii. Lines or substations built close to the sea where the salt level in the air might increase the risk of equipment damages;
        iii. Line or substation built in very dry or desert area where temperature and sand storm might increase the risk of equipment damages.
    b. design conditions;
        i. design choices of substations like outdoor or indoor substation, air or SF6 isolated substation, might change the probability of occurrence of the fault;
        ii. activation of Special Protection Scheme, which by definition will cause sudden disconnection of multiple grid elements.

[6] The initial design of the equipment generally takes into account these specific conditions. Nevertheless, during its whole life, those conditions can evolve or the design can appear insufficient with consideration of the actual conditions of the specific location.

2. Temporary occurrence increasing factors, as example:
    a. operational conditions
        i. Depending on the substation design choices, the probability of a busbar fault may be increased during maintenance period;
        ii. Depending on the design choices, the probability of a multiple cable fault in same trench or multiple lines fault on same tower may be increased during work in the vicinity;
    b. weather or environmental conditions,
        i. Depending on design and technical choices, loss of multiple lines due to tower incident or busbar fault may be increased during severe weather conditions or environmental conditions e.g. threats of flooding, forest fires.
    c. life time or generic malfunction affecting risk of failure
        i. Aging material are subject to decreasing reliability which can increase probability of failure until replacement;
        ii. Generic malfunction can affect material which thus proves less reliable than expected.

These examples are not exhaustive and illustrate that the conditions of application of each of these criteria are strongly depending on the design choices and technical specifications which are and have been done when developing the grid. They will have to be addressed individually by each TSO for its grid as required by CSAM Article 8 taking into account operational or weather conditions in relation with the specifications and the current state of the equipment and where available the history of incidents that occurred on the concerned grid elements.

Impact of contingencies

In addition to previous criteria related to the probability, it is also possible to consider criteria related to the impact, in accordance with Article 33 of SO GL. Impact means consequences but also remedial actions to cover them. Indeed, some exceptional contingencies, even with a low probability, due to the historical grid design choices or design constraints (e.g. geographical or environmental constraints leading to a structurally weak system, such as long lines or not enough meshed) may have a high impact, over the level of the local consequences which are considered as acceptable by TSO's national rules. Such a situation can lead the TSO as required by CSAM Article 10(1.d) to take into account these contingencies in order to avoid this kind of unacceptable consequences. However, such consequences should only be covered if the cost of necessary remedial actions is deemed proportionate to the risk, with respect to a very low probability of occurrence.
In addition, exceptional contingencies may also lead to cross border high impact and should thus be taken into account and coordinated at inter-TSO level. In this case, CSAM Article 9 provides that affected TSOs may agree on exceptional contingencies to be included in their contingency list provided that they agree on the contingencies to cover and the maximum cost of remedial actions to cover them while ensuring that all affected TSOs are part of the agreement. TSO shall have to apply the following process to establish such agreements:

- TSO A identifies an exceptional contingency with high cross-border impact which is located in TSO B's control area and has consequences in TSO A's control area.

- TSO A and B identify all the other TSOs affected by this contingency either because the contingency itself has consequences for those TSOs or because the remedial actions required to cover this contingency are cross-border impacting for those TSOs.
- TSO A, TSO B and all the other affected TSOs agree on the conditions where such an exceptional contingency will be covered, notably the maximum cost of remedial actions above which cost of fulfilment of operational security limits shall not be deemed proportionate to the risk.

However, some ordinary contingencies, even with a high probability, due to the historical grid design choices, shall never have consequences which are considered as inacceptable in respect with TSO's national rules. In such situation CSAM Article 10(4) provides that the TSO, in order to reduce computation time and simplify the analysis of the results, may decide not to take into account these contingencies in his contingency list (examples: loss of small grid users, small reactors, small capacitors...) provided those contingencies are not part of the contingency list of another TSO.

Exchange of information with neighbouring TSOs

It is also of the upmost importance that TSOs inform in due time all electrically neighbouring TSOs (as defined in the Influence chapter) about changes in the contingency list which concern grid elements being part of the observability area of those TSOs. This information shall allow those TSOs assessing whether or not these new or updated contingencies shall be part or not of their external contingency list of these TSOs. The process for ordinary contingencies is described in chapter 3.
However, the identification of external exceptional contingencies requires a TSO to be informed by its electric neighbours of the exceptional contingencies that they identified in application of the probability criteria. Some exceptional contingency may be covered only when operational conditions are met (e.g. weather conditions). In this case TSOs may be informed by a neighbouring TSO that it covers an exceptional contingency with short notice and have little time to assess whether they should also cover it. That's why CSAM provides a two-step process for sharing potential exceptional contingency lists:

1. In advance, TSOs share their potential exceptional contingencies to identify if they may endanger their grid.

2. Then, when operational conditions are met, a given TSO includes in its contingency list an exceptional contingency and informs concerned TSOs, then those TSOs include it in their contingency list (as an "external contingency") if it has been identified previously as being able to endanger their grid.

Of course, for permanently covered exceptional contingencies there is only one step: TSOs share their permanent exceptional contingencies to identify if they may endanger their grid and if so, cover them.
There is no need for a process to share exceptional contingencies with high impact since they are jointly identified.

Towards a probabilistic risk management process

According to Article 75 of SO GL, TSOs should develop common principles for risk assessment, at least covering probabilistic approach for what concern the consideration of contingencies. Without questioning the fact that this will remain the final target, the rules provided by CSAM are not based on a top-down approach where a probabilistic assessment of risk will be applied by each TSO and a harmonized threshold for acceptable risk would be defined. CSAM provides qualitative rules to

reflect the differences in the probability of occurrence of contingency that will have to be consider in the N-1/N-k principle based on a bottom-up approach which is reflecting current practices for TSOs in Europe but also around the world. This approach acknowledges that a strict respect of Article 75 requirements is not achievable in the short-term as methodologies based on full probabilistic approaches are not mature and/or experienced enough to be translated into requirements for TSOs that will have to be applied in operational processes.
TSOs recognize that, in the recent years, progresses towards full top-down probabilistic and/or risk based processes for common security assessment in operational planning and in real-time activities (as referred to in article 75 of the SO GL) have been achieved in different national or European R&D initiatives in which TSOs have been deeply involved (e.g.: iTesla, Garpur, Umbrella…and especially for what concern the conceptual, algorithms and tooling aspects). Nevertheless, these initiatives have also reported that there are still important topics and questions that require additional R&D and/or demonstration activities before becoming mature enough to be translated into pan-European operational requirements. Among these topics we may highlight

(i) the principles identifying the collection of data and the related methodology to provide correct evaluation of the density function of the possible grid situations and of the probability of occurrence of contingencies, especially the exceptional ones;
(ii) the effective availability of sufficient historical data to estimate these probabilities for each situation and each contingency
(iii) the impact assessment on the cost/benefit and on the TSO management endorsement of such significant changes in the way to assess the security of the system, taking into account differences between TSOs/countries in historical grid design choices (i.e. tower design vs wind withstanding capability, different design of substation,) or in risk management.

Considering the above, CSAM Article 43 provides that TSOs will describe and lay down the steps necessary for a potential transition towards a probabilistic risk assessment through periodical reports and will start defining and implementing a process for the collection of the relevant data.

4.5 Remedial actions to coordinate

Timescale for the activation of remedial actions

During operational planning processes (from year-ahead to close to real-time) security analyses are performed with the respective grid models. In case some violations of operational security limits are detected (in N or when a contingency is simulated), the responsible TSO(s) has/have to prepare remedial actions to ensure security of supply for the real-time situation. In case the TSO(s) might not be able to prepare and activate this remedial action in a timely manner after a contingency occurs to prevent any limit violations in the system - e.g. long lead times for re-dispatch of power plants – remedial actions have to be activated prior to the potential occurrence of the contingency and to the investigated timeframe for compliance with the (N-1) criterion. Those remedial actions are defined by CSAM as Preventive Remedial Actions (PRA) and are planned binding once agreed - unless not otherwise agreed later - but are activated as close as possible to real-time (Art 21.2.b of SO GL). In case the permanent admissible transmission loading (PATL) of equipment is violated but not the transitory admissible transmission loading (TATL), there might exist a timeframe of several minutes within which the TSO(s) is/are able to prepare and activate a remedial action in a timely manner - e.g. change of PST settings, manually or automatically - to prevent any limit violations in the system. Those remedial actions are defined by CSAM as Curative Remedial Actions (CRA) and are activated straight subsequent to the occurrence of the respective contingency for compliance with the (N-1) criterion.

After the occurrence of a contingency there should be no violations of operational security limits in the transmission system, as all TSO(s) has/have to comply with the (N-1) criterion and has/have activated either preventive or curative remedial actions. Nevertheless, after such an occurrence, the transmission system may be now in 'alert state', means a system state in which the system is within operational security limits, but it exists at least one other contingency from the contingency list for which, in case of its occurrence the planned remedial actions, if any, would not be sufficient to prevent operational security limit violations. Therefore, the transmission system is no longer (N-1) secure. Also, an unforeseen change in the electrical situation through, for example, forecast deviations, can lead to (N-1) violations without any occurrence of a contingency. TSO(s) shall activate in those cases a remedial action in order to ensure that the transmission system is restored to a normal state as soon as possible and that this (N-1) situation becomes the new N-Situation (Art. 35 SO GL). Those remedial actions are defined by CSAM as Restoring Remedial Actions (RRA).

It shall be noted that PRAs and CRAs are planned during the operational planning phase, whereas RRAs are elaborated and decided in real time.

Identification of remedial actions to coordinate

Due to the system physics, any action applied by a TSO on its control area will theoretically influence voltage and flows of the whole synchronous area. Fortunately, in most situations, the effects of those actions are restricted to a small perimeter outside of which their effects remain below the level of natural stochastic variations of the system. However, such a perimeter of measurable effects may comprise grid elements from another TSO's control area. When the system is operated close to its limits, in absence of coordination between TSOs, an action applied in one TSO's control area may have an unforeseen and negative impact in another TSO's control area that may lead to global consequences. TSOs must therefore identify which remedial actions require coordination before being implemented.

The following Figure 12 shows the simplest case of cross-border impact: to solve a constraint on an element from its control area, TSO A needs to apply a remedial action located in its control area that has a high influence on an element from TSO B control area. The application of such a remedial actions has to be coordinated between TSO A and B. TSO C has not such influenced element in its control area and shall not be involved in the coordination of the application of this remedial actions.

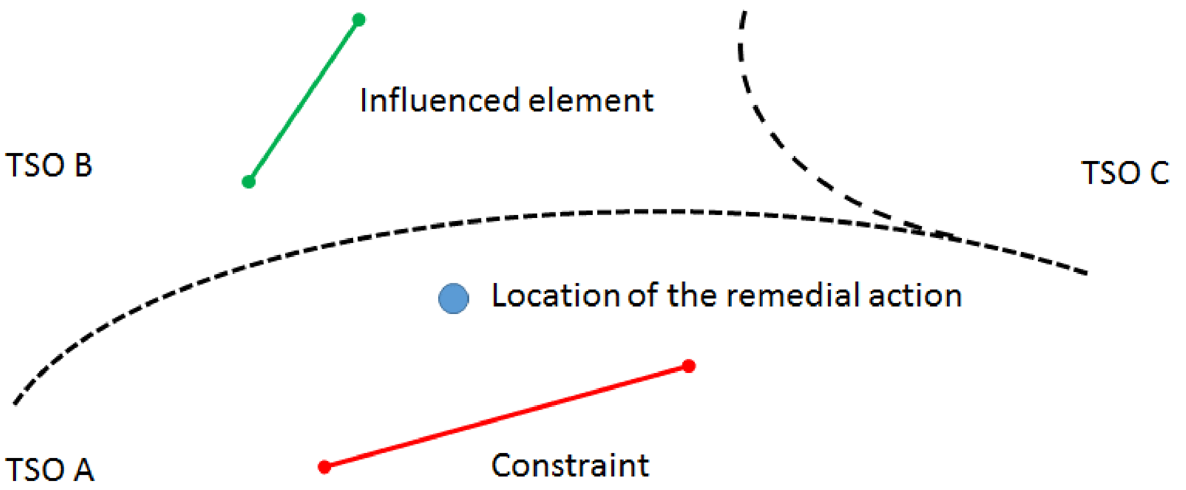


Figure 12

ENTSO-E AISBL • Avenue de Cortenbergh 100 • 1000 Brussels • Belgium • Tel + 32 2 741 09 50 • Fax + 32 2 741 09 51 • info@entsoe.eu • www. entsoe.eu

The cross-border impact of a remedial action is not the same thing that the character of cross-border relevance of a congestion. Indeed, a remedial action (e.g. a PST tap change) considered by one TSO for solving an internal congestion, due to internal flows only, may have cross-border influence on other TSOs control areas. On another hand, a congestion on a grid element of this TSO, due to cross-border flows (loop-flows, transit or export flows) is a cross-border congestion, but in some cases, this congestion can be removed by a remedial action within this TSO control area, without any impact on flows on other grid elements outside its control area. This remedial action will not be a cross-border impacting one, but, if costly, will clearly be subject to cost-sharing agreement, as it solves a cross-border congestion.
In the case of such cross-border congestion, CACM Article 35 and SO GL Article 76 sets the need for TSOs to develop common proposals, at CCR level, in order to:

- identify on which grid elements operational security limits violations shall be treated as such,
- define the remedial actions of cross-border relevance (eg: kinds, locations, minimum efficiency…) which shall be managed in a coordinated way to remove such violations,
- identify the remedial actions of cross-border relevance which are the most effective and economically efficient one for a given violation.

As a result, the definition of processes to identify coordinated remedial actions aimed at solving a cross-border congestion, more detailed than existing requirements set out in SO GL is out of the scope of the CSAM and is to be dealt with in regional proposals (SO GL Article 76 and CACM Article 35). Nevertheless, some common general principles to be taken into account by all TSOs when developing these Article 76 proposals, or applied by all TSOs are provided in CSAM articles 15 to 21 (see below).
Among these principles, CSAM Article 20(3) requires that the regional process needed to achieve the agreement on a cross-border impacting remedial action, envisaged by a TSO or by a RSC, shall be consistent with the regional process needed to achieve the agreement on a remedial action of cross-border relevance.

Note also that CSAM scope does not cover the definition of cost sharing rules for costly remedial actions (SO GL Article 76 and CACM Article 74).

Determination of cross-border impact

Regional operational security coordination and thus coordination of remedial actions (being cross-border impacting remedial actions or remedial actions of cross-border relevance) will be performed in accordance with methodologies developed in application of SO GL Article 76.
CSAM Article 15 provides requirements for identifying which remedial actions a TSO shall identify as cross-border impacting, thus needing to be coordinated before being decided to be applied. This is done in two steps:

- Determine ex-ante which remedial actions should be or should not be coordinated
- For the other remedial actions not ex-ante classified, provide ways to determine if they should be or should not be coordinated.

Cross border impact of remedial actions may be assessed by quantitative or qualitative assessments. Qualitative assessments are simpler but remain mainly empiric and it seems not always feasible to justify a good trade-off between cross-border impacting and non-cross-border impacting remedial actions resulting from the only application of qualitative criteria. Quantitative assessments aim at assessing the actual influence as a change on flow and/or voltage on grid elements from other TSOs control areas resulting from the application of the investigated remedial action. With respect with the different ways they are applied, such quantitative assessment shall be performed:

1. On the N and (N-1) situations for preventive remedial actions
2. On the (N-1) situations for which they are considered for curative remedial actions

By default, CSAM provides a formula in Article 15(1) . This formula assesses the change of flows, and as an option of voltage, resulting from the application of a remedial action and has the following properties:

- The influence of a remedial action can be assessed by a TSO on its own which is especially useful when a remedial action is designed during a coordinated operational security analysis performed by the TSO in operational planning or on a state estimation in real time operation,

- a remedial action that does not change the set point of an HVDC system connecting two synchronous areas has no influence on another synchronous area.

Moreover, RSC are not required to assess the cross-border impact of a remedial action that it proposes since, by default, such a remedial action is to be agreed by affected TSOs, according to Article 78(6) of SO GL.
CSAM also provides a default threshold in Article 15(6) for TSOs to assess whether a remedial action shall be deemed cross-border impacting. This threshold has been derived from current TSOs practices. Throughout Europe, a change of flows in a range of 50 to 100 MW in absolute is deemed significant enough so that it has to be coordinated. That's why a relative change of flows of 5% of PATL has been proposed as a default threshold assuming an average capacity for a 400 kV line of 1,500 MW. This threshold may be decided as at CCR level to adapt to regional specific situations.

Remedial actions coordination

Cross-border impacting remedial actions shall be subject to coordination having in mind that

- The higher the number of cross-border impacting remedial action is, the more complex will the coordination process be,
- If there were no coordination at all, TSOs would have to apply increased security margins to avoid that non-coordinated remedial actions implemented by other TSOs endanger their grid.

Therefore, CSAM Article 17 provides that:

- Coordinating a remedial action means to inform affected TSOs about the reasons why this remedial action is designed and ensure that all those affected TSOs accept its implementation.
- Preventive and Curative Remedial Actions that are deemed cross-border impacting have to be coordinated
- Restoring Remedial Actions that are deemed cross-border impacting have to be coordinated when the system is in alert state
- Restoring Remedial Actions that are deemed cross-border impacting have to be coordinated only when operational conditions allow it when the system is in emergency state

This approach allows to adapt the coordination to the criticality of the situation: as long as the system remains in normal state or alert state, only the occurrence of a contingency may endanger the grid whereas when the system is in emergency state remedial actions may have to be implemented quickly to prevent the system from collapsing.
In addition, Article 19 provides some requirements on the operational application of the principles setup in SO GL regarding the timings of application of the remedial actions on the electrical system. However, this article provides flexibility to anticipate the activation of preventive remedial actions as long as this does not endanger the grid. Indeed, in some quickly changing situations, such as mornings where several planned outages must start around the same time or when market conditions lead to huge change of flow, operators in control room may not have time to implement all the remedial actions required in a short time. Implementing remedial actions earlier discharges operators from those peaks of workload and allows a more secure operation of the system by reducing the stress and thus the probability of human errors.

Consistency of the different proposals pursuant to Article 76

In order to achieve the needed consistency between the different proposals for regional coordination required by Article 76 of SO GL, while leaving enough flexibility for each of them to address regional specific technical issues and organisation, CSAM defines in Article 20 some fundamental elements which have to be defined/taken into account in/by each of these proposals, such as: define the grid elements to be monitored, how to take account of previously agreed remedial actions, what shall be the outputs of the process and what it shall ensure at least in terms of coordination.

Finally, in order also to achieve consistency of practices among all TSOs:

- Article 18 provides principles regarding which remedial actions shall be deemed available by a TSO for regional coordination purposes
- Article 21 provides principles to clarify which activities can be done by a TSO to prepare IGMs and to define which remedial actions can/shall be included in these IGMs;

5. Uncertainties

5.1 Introduction

Coordinated operational security analyses deal with the identification of risks on the interconnected system of operational security limits violations, trying to find the appropriate remedial actions, according to SO GL Article 21, and ensuring the coordination of these remedial actions. According to SO GL, these analyses are done on a common grid model in the operational planning phase.
Uncertainties may have a visible effect on these coordinated operational security analyses, since in some cases operational security limits violations, which were not previously identified may arise in real time, or remedial actions prior agreed may not be enough or on the contrary may not be necessary any more. This methodology handles uncertainties in order to reduce these undesirable effects.

5.2 Uncertainties: what are they, what is their impact on operational security analysis?

TSOs must face different sources of uncertainties that affect coordinated operational security analysis results: uncertainties regarding injection that can appear in the demand or in the generation, uncertainties related to the market and finally other uncertainties such as the forced outages, effective topology, dynamic line ratings, values decided based on weather conditions, etc.

Generation

Uncertainties related to renewable generation have an impact on coordinated operational security analyses, the greater when insufficiently forecasted. This kind of intermittent generation depends heavily on weather conditions so the output generation is highly variable and can originate very diverse scenarios. In this sense, the great challenge for renewable energy forecast is precisely predicting sudden changes in power generation, since an unforeseen ramp-down or ramp-up in renewable generation can become a challenging difficulty to cope with for the system. Since installed renewable generation is increasing in almost all countries, the effect of this kind of uncertainties is becoming more and more relevant.

Time horizon has a significant influence in these uncertainties since the forecast error is drastically reduced for the first hours. There is also an important influence of the area size analysed, since this generation depends heavily on weather conditions, forecast error increases for small areas while when aggregating a whole country production, the forecast error decreases significantly.

Demand

Demand vary significantly from one moment to another, nevertheless daily, weekly and seasonally patterns can be established. Even though these patterns can be forecasted, there are also other factors that can influence demand such as weather conditions consequently any error in weather forecast will be transferred to demand forecast; other factors like particular events (holidays, strikes...) equally affect these patterns.
There is also a source of uncertainties in the reactive part of demand due to high variability of reactive load and effects of DSO compensation procedures. Nodal allocation of load on nodes represented in the data model, resulting of an aggregation process also generates active and reactive uncertainties. Whereas reactive power uncertainties can be quite significant, their main impact is local, therefore it is not covered in this methodology.

ENTSO-E AISBL • Avenue de Cortenbergh 100 • 1000 Brussels • Belgium • Tel + 32 2 741 09 50 • Fax + 32 2 741 09 51 • info@entsoe.eu • www. entsoe.eu

Although load has been a traditional source of uncertainty in the past, nowadays load forecasting is considerably more accurate as a result of TSO's experience and also recurring and predictable patterns in load profiles. Uncertainty levels nevertheless increase significantly with the time horizon, notably for areas with high dependency of load on weather conditions. Load forecast accuracy is significantly better at aggregated level (region, country) than at nodal level. In the future, load forecasting is expected to become more difficult because of the volatility which will be introduced by emerging paradigms, such as demand response growth, EV charging etc. They are not captured in the current version of CSAM.

Market uncertainties

A source of uncertainty can be identified for horizons greater than the difference between real time and last intraday gate, since market participants try to reduce their expected imbalance or maximize their profit by playing on the intra-day markets (cross-border or internally), making the schedules of dispatchable generation more difficult to predict the day ahead or in intraday far from the real time.

Other uncertainties

Another source of uncertainties are incidents that can occur in the transmission grid such as the tripping of elements: lines, double circuits or busbars. These events cause unforeseen changes in the topology of the network which will affect the results of the security analysis.
Finally, as coordinated operational security analyses are run on common grid model, built in day-ahead or intraday for short-terms studies, it is also essential that TSOs avoid any additional uncertainties on the results which happen because of mistakes in the individual grid models used to build CGMs, e.g. on preferred topology, planned outages inclusion, inclusion of already agreed preventive remedial actions…

5.3 Objectives of security analyses

In the operational planning phase, security analyses are run in order to:

- Identify the capability of realizing the simultaneous planned unavailability of assets, including design of remedial actions to facilitate them
- Evaluate the expected capability of the system to respect the operational security limits in the N situation or after the simulation of one contingency of the contingency list, including design of remedial actions needed to remove identified constraints

Those studies are run in two main timeframes, long-term typically from year-ahead to week-ahead (potentially up to D-2) and short term from day-ahead towards intraday.
The methodology focuses on the conditions required to realize those coordinated security analyses, in addition to requirements provided in SO GL. Coordinated SA are needed as soon as impacts on the interconnected system are evaluated. According to SO GL, those coordinated security analyses can be run by a TSO or by an RSC (on a regional perspective). In all cases, they shall be done on a CGM and remedial actions shall be coordinated where they have cross-border impacts.
In the long-term, TSOs face a lot of uncertainties (e.g. no market position; no forecast of weather-dependant RES; weather impact on long-term trends such as hydro generation level; unplanned long-lasting forced outages…). Hence, they assess the system security on the basis of scenarios, either representative of average situations or of more severe ones. Although the uncertainties are relatively high, those studies are necessary to ensure needed long-term processes (outage planning, long-term

ENTSO-E AISBL • Avenue de Cortenbergh 100 • 1000 Brussels • Belgium • Tel + 32 2 741 09 50 • Fax + 32 2 741 09 51 • info@entsoe.eu • www. entsoe.eu

capacity calculations) or prepare in advance measures to face expected risks. In general, in such a long-term, remedial actions are assessed as needed (e.g. choice of a given topology) but they are not yet decided definitively.

In the short term, the degree of uncertainty tends to decrease, e.g. RES inputs can be forecasted, load forecasts are quite accurate, generation location and level is available through scheduling processes, … Nevertheless, at a given time ahead of real-time, a level of uncertainty always remains, notably the effects of forthcoming intraday market activities, forecast errors, forced outages...

The objective of coordinated security analyses in the short-term is to assess the security of the system on the coming hours of the day (ideally continuously, in practice on e.g. hourly timestamps) more and more precisely, to fine tune the need for RA and their design, including coordination, and to decide their application at the latest taking into consideration their needed activation time. This means that security shall be reassessed sufficiently frequently, or when a special event triggers the need for a reassessment. In terms of regular updates of the security assessment, there is no uniform answer across Europe either in terms of frequency or of most adequate timings. This depends on multiple issues such as intra-day market activity, RES impact on flows, RES and load forecast accuracy, time needed to activate remedial actions.

In the short-term period, agreed remedial actions are implemented the closest to the real time, taking into consideration the delay to activate them (which can be up to 24 -48 hours for some plant start-up). As these decisions are taken based on data affected by uncertainties, an appropriate balance must be adopted between:

- Using conservative margins to avoid any risk of not-anticipated constraint, at the cost of increasing the number and costs of needed remedial actions; this is specially impacting when the kind of constraint requests the use of costly remedial actions on generation to be implemented long before real time –due to 24-48 hours delay- where uncertainty levels are still relatively high. Moreover, as this kind of conservative decision can be judged in real-time finally not necessary, if this happens regularly, this can lead to a loss of confidence in the studies and decisions made in the operational planning phase;
- Using less conservative margins with the risk of facing constraints identified only closer to real-time with limited available remedial actions solutions (due to the fact that some are no more available), ultimately leading to the risk of N-1 security violation.

5.4 Managing Uncertainties

As described previously, the handling of uncertainties is an issue for TSOs to address, and is a challenge to be managed in processes in all timeframes of operational planning. This is indeed a wider question as it also concerns work areas such as network planning, asset management, and market design.

Based on varying conditions and area of application, various strategies for addressing uncertainties have been developed. Below follows a description of the strategies considered as possibilities to address the requirements for assessing and dealing with uncertainties, notably of generation and load in the context of SO GL:

Use more stressed values than the forecast

This approach consists in replacing the expected value (or reference value such as the average) by another one which allows one to stress the system and therefore will prevent missing the detection of unsecure situations resulting from underestimation of injections. General advantages with this method are related to providing more secure results and ease of implementation for analyses whilst the challenges relate to preparing scenarios combining different stresses and the interpretation of results, notably with respect to the decreasing probability of the more stressed values. A further risk with such an approach is that it may lead to increased volumes of remedial actions to be activated which after the fact may prove to have been unnecessary.

Use margins on results

This approach, in general, consists of keeping a margin when evaluating the results of the security analysis in order to secure the evaluation against effects of uncertainties. A simple method is to evaluate the violations of operational security limits by applying a constant security parameter on those limits: for example, checking computed flows against PATL or TATL reduced by 5%, or applying a statistically calculated margin per branch. The advantage with an approach using margins is that an approach can be developed to be similar in application and interpretation as reliability margin in capacity calculation. The disadvantages are related to the complexity and data requirements for the statistical analysis as well as the fact that the intuitiveness of results may not be compatible with operational processes for short term studies. A further disadvantage is that the approach may, as with using "stressed values" lead to an increase of volumes of remedial actions to be activated, which after the fact may prove to have been unnecessary.

Examine sensitivity of results

This approach is based on a full probabilistic description of input variables and possible events to evaluate the probabilistic expectation of N-1 violations or alert/emergency state. Such a method may be advantageous as results showing which contingencies have the highest probability to cause violations can displayed and which could be made even more useful, if combined with severity index, as a tool for decision making in preparing remedial actions. However, such a probabilistic approach is not in line with the current dominance of deterministic methods, and therefore there is also a lack of tools, data and understanding for such an approach to be implemented by all TSOs in the medium term of several years.

Use "best forecast" values combined with update requirements.

The "best forecast" values method consists of the utilization of the best available forecast value for the injections. It is the classical method, mostly used by all TSOs. The best forecast value is either the result of a forecast model (mainly for day-ahead or intraday studies) or is a fixed value, normally equal to the average value for the studied day. In order to properly manage the effects of uncertainties of generation and load using best forecasts it is important that the forecasts are updated at a sufficient frequency to make sure that changes in the forecast that may affect the results of security analysis is captured. The advantages of a "best forecast" approach are that it is a well-known and proven approach and that the results are suited for process constraints and are sufficiently simple and intuitive to be easily analysed in short term studies. The disadvantages of such an approach are obviously related to the accuracy of forecasts and this approach is therefore not suitable for timeframes longer than D-1 or D-2. Such an approach obviously is less robust than other approaches which consider margins or more stressed situations, but therein also lies the advantage that it seems reasonable that remedial actions are only set up when operational security violations are identified based on best available forecasts.

It is worth noting that only the last two approaches (probabilistic and "best forecast") are not introducing a "risk aversion" bias.

Suggested approaches

As the requirements in SO GL is focused on operational planning from year ahead to real time operation it is important to mention that, in addition to achieving a balance between being too conservative or risking security violations as mentioned in the section Roles and organisation of security analysis in operational planning, choosing of a strategy for assessing and dealing with uncertainties of generation and load must necessarily consider the following aspects:

i. what are the current/expected operational process/es
ii. capabilities of existing tools
iii. availability of data required
iv. timeframes in which processes must be completed
v. the need for operators to make decisions based on the results and therefore the intuitiveness of the results, including their appropriateness a posteriori, which drives the confidence put by operators in the decisions made in the operational planning phase.

Choice for Long Term studies

The chosen approach for long term studies is that the scenarios which shall be used as a basis for the long-term security analysis studies, described in Article 72(1)(a) or (b) or for outage coordination following Articles 98(3), 100(3) and (4), are the scenarios required according to SO GL Art 65.

However, these scenarios can be seen as average or fixed observed values and would therefore not sufficiently cover uncertainties to allow studies such as those required for outage coordination. For example; how would three TSOs combine their needs where TSO A would require a scenario with low wind infeed to be studied to be assured that a line may be put in maintenance for a longer period of time, whilst TSO B may require to study a situation with high hydro infeed for some time during the same duration, and even TSO C needing to study a situation with high wind infeed. Extrapolating this problem to all European TSOs would of course not be a sustainable solution.

The suggestion is therefore to allow local scenarios, letting each TSO decide for which operational planning activities those local scenarios are to be considered, in addition to the common scenarios mentioned above, and shall inform the TSOs of its capacity calculation region or of its outage coordination region and the relevant RSCs about the content of those local scenarios and their usage purpose. This is similar to the existing requirement in SO GL Art 80(3)(c) for TSOs to provide the regional security coordinator with scenarios to detect and solve regional outage planning incompatibilities, but an extension. To cover these scenarios with IGMs from all TSOs and consequently CGMs could potentially results in an unmanageable number of IGMs/CGMs. Therefore, all TSOs shall not be required to create an IGM per local TSO scenario, but rather the requesting TSO should define, in coordination with other TSOs of the concerned capacity calculation region, which grid models shall be used to study these local scenarios. Furthermore, these grid models shall be derived from the common grid models established pursuant to SO GL Art 67, using appropriate substitutes or derived models where appropriate.

In this way sufficient stresses can be applied locally to ensure an acceptable level of confidence in the security analyses studies whilst maintaining coordination and commonly agreed scenarios.

Choice for short term studies

The chosen strategy in this methodology is to consolidate on the basis of proven stable solutions, namely combining using best forecasts with specific requirements on regular updates of the forecasts, considered along with the requirements which TSOs are to fulfil in the application of CACM and SO GL.

The strategy can be summarised such that each TSO shall perform 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:

- Considering that a margin in line with Article 22 of Regulation (EU) 2015/1222 shall be already taken into account for capacity calculation processes (in a context of large uncertainties and big approximations, with the goal to offer firm capacity to market participants whatever happens after), whereas the goal of the operational security analysis is fully different and is to identify expected operational security limit violations and consequent needed remedial actions, each TSO shall not take into account any reliability margin to its operational security limits when evaluating the results of the coordinated operational security analysis. In the same way, each TSO shall not include in its day-ahead individual grid models any reliability margin to the operational security limits.
- Individual grid models and subsequent common grid models, created in the application of Article 70(2) of SO GL and according to the methodology of Article 70(1) of SO GL, shall include load and intermittent generation forecasts established on the basis of the latest available forecasts for load and intermittent generation built according to CSAM Article 37 and Article 38. The detailed requirements for forecast updates are discussed in more detail in section 5.5, but these requirements are aimed at handling the uncertainties related to specifically intermittent generation and load.
- Individual grid models and subsequent common grid models, created in the application of article 70(2) of SO GL and according to the methodology of Article 70(1) of SO GL, shall also include market results, schedules, and planned topology of the transmission system. This article of SO GL already requires TSOs to provide updated inputs where market results and consequent generation schedules are available –they are expected to be accurately provided by market participants, and at the right level of granularity needed by the TSO, on the basis of the application of SO GL articles 40 to 53-, as well as it requires the TSO to provide an updated forecast of its grid topology.
- Agreed remedial actions (or unilaterally decided by TSOs, when they are allowed to do so) shall be included in individual grid models and subsequent common grid models as required in Article 21 of CSAM. This requirement implies that TSOs shall include all remedial actions, including countertrading and redispatching in IGMs, thereby reducing this source of uncertainty and allowing for this to be accounted for in subsequent analysis.

For D-1 security analysis specific synchronized timings are also set for coordination to allow all TSOs and RSCs to work on data established at the same moment.

For the intraday timeframe specific requirements are set in the CGM methodology developed pursuant to Article 70(1) as to the minimum number of IGM updates in, which will enable all TSOs and RSCs to perform their security analyses on the basis of these updates. On top of that, notably in the regions which these minimum global update forecasts are seen as not sufficient with respect to the variability of the forecasts, eg due to high level of RES or very active intraday markets, TSOs are further required to determine additional IGM updates frequency and the corresponding frequency of intraday coordination of operational security analysis, per CCR, by application of SO GL Art 76-77.

Any approach which is based on forecast updates is also dependant on monitoring of the results and implementing corrective actions where this is required. This is covered by monitoring tasks required in SO GL. SO GL Articles 15(4) (b) and (d) require reporting of events which have occurred due to forecast discrepancies. In addition SO GL article 17 (2) (b) requires reporting from the RSC on events, remedial actions and cost. In addition to these requirements for reporting, Article 70 (5) of SO GL also requires each TSO to assess the accuracy of the variables specified in 70 (3), and then corrective actions in accordance with Article 70 (6) of SO GL in case of the TSO assesses this accuracy is not sufficient.

With consideration to the expected continuation of a regular increase of the impact of uncertainties, mainly those resulting of RES/load injections and of intraday internal and external trades (up to the gate closure), TSOs also identify the selected approach (best forecast and sufficient updating frequency) could become insufficient in the coming years and there may be a need to study an enhanced approach using margins when analysing the results of security analysis (and consecutive remedial action decisions) run several hours ahead of real-time. This is however not the current choice described in the present CSAM but could be foreseen in future evolutions of the methodology. At least CSAM article 39 requires to regularly review the adequacy to the needs of the minimum frequency for providing IGMs updates by all TSOs which are defined in the CGM methodology.

Handling of specific weather risks or other exceptional not planned event

When a TSO expects exceptional situations to be faced, resulting from out-of-range contingency (e.g. destruction of several assets after a windstorm), its general behaviour is to analyse in advance what could be the consequences of such events, and coordinate with potentially concerned TSOs, either because they could be affected or because they could help to face the situation. In some cases, the time needed to come back to normal state can be long, up to several days/weeks. The requirements set up in CSAM article 25 are established to ensure a consistent approach of all TSOs in that type of situations.

5.5 Forecast updates principles

Setting a definitive target in terms of maximum error which should not be exceeded is an unachievable objective, since there is a lack of definitive basis on which it can be based. For example it cannot be simply compared to the reserves needed for facing the reference incident for generation disconnection, because this event is sudden and located in one node, additionally defining a maximum error to be compliant with could lead to difficulties since predictability of intermittent generation, and also load, is very variable in different zones of Europe depending on the instability of weather conditions; being more difficult to remain below the maximum error for certain zones.

The empiric target which has been taken into account to determine forecast update requirements is to avoid that lack of adequate forecast would lead to errors due to RES greater than an order of 2-4 % of the reference load for each control area. This value is in the magnitude of observed errors on load forecast, and can be deemed as adequate, as experience shows that it can be managed by TSOs.

Requirements are defined with respect to the "reference load" of each control area. This reference load in the following has been taken as the average load (total consumption energy (in MWh) in the control area divided by the number of hours in the year).

Forecast updates of intermittent generation

Requirements are different according to level of installed intermittent generation in order to maintain the level of error of 2-4% of the reference load.

As regard the types of intermittent generation subject to requirements on forecasts, the requirements concern only the intermittent generation types which are highly sensitive to rapidly changing weather conditions from one hour to another one in the same day. Slower varying level of intermittent generation (e.g. run-of river hydro) are not subject to those requirements as it is expected that their slow variations are sufficiently anticipated and compensated. This means that the following requirements apply only to wind and solar generation. It could be extended in the future if other weather sensitive technologies of intermittent generation would develop.

As regards wind or solar generation forecast, current experience shows that their forecast depends firstly on the weather forecast, those forecasts can be improved by the use of multiple tools and can be strongly improved for forecasts of several hours ahead if an estimation of actual generation is taken into account in the forecast algorithm. Due to the fact that weather forecast is updated twice a day at Pan-European level, requirements based only on weather forecast must not exceed this frequency. As forecasts can be strongly improved if real time measurements or estimation of actual generation are taken into account in the forecast algorithm, in the case of a high level of RES installed capacity estimation of actual generation is included in the requirements in those cases in which it has been verified that the use of this estimation improves forecast accuracy. It may also be the case that it is not feasible to obtain real time measurements, for example in the case of PV on roofs.

There is no requirement of forecasts updates for those TSOs with a level of intermittent generation less than 1% of the reference load, since until this level of generation there is a non-relevant effect in transmission system from this source of energy.

TSOs for which the level of intermittent generation in their control area is "moderate" (defined from 1% until 10% of the reference load) must have at least a forecast available for each hour and established once a day. Errors in forecast for the 24 hours horizon can typically reach up to a maximum of 20% of installed capacity that could involve errors of up to 2% of the reference load.

TSOs with a "medium" level of intermittent generation installed capacity in their control area (defined from 10 to 40 % of the reference load), must have at least the forecast updated 2 times in intraday; errors in forecast for the 12 hours horizon are thus reduced and can typically reach up to a maximum of 8% of installed capacity which could involve errors of up to about 3% of the reference load.

TSOs with a "high" level of intermittent generation installed capacity in their control area (above 40 % of the reference load) must have forecast updated every hour taking into account real time measurement or at least estimation of generation provided it has been verified that the use of this

ENTSO-E AISBL • Avenue de Cortenbergh 100 • 1000 Brussels • Belgium • Tel + 32 2 741 09 50 • Fax + 32 2 741 09 51 • info@entsoe.eu • www. entsoe.eu

estimation improves forecast accuracy. Errors in forecast are thus further reduced for the 1 hour horizon.
In summary one could say that the increase in forecast frequency in relation to installed capacity is aimed at creating a good balance between costs incurred for establishing forecasts whilst aiming for a level of security achieved by keeping the expected error to within 4% of average load. This balanced approach is in line with SO GL Article 4(2) requesting a principle of optimisation between costs and overall efficiency in its implementation.

Forecast updates of load

Requirements of load concern only active power since although reactive power uncertainties are quite significant, their main impact is local so is not covered by this methodology.
The parameter selected to determine the frequency for updating load forecast has been load's temperature dependency. The chosen value has been a MW/ºC gradient greater than 1%, since weather forecasts is usually accurate to within +/- 2ºC, which could imply a variation of load of 2%, in line with error level established. It should be stressed that although the gradient of the load's temperature dependency has been selected as the parameter to determine the requirement for the frequency for updating the load forecast, this value has been selected as a common criterion for all TSOs of primary importance. It is therefore still the responsibility of each TSO to include other information required to establish an accurate load forecast. Examples of other information could include: meteorological data such as cloud cover or precipitation; information from market participants such BRPs; demand side response or the price elasticity of the load.

6. RSC Coordination

This part of the supporting document deals with Art 75(1)(d) which requires all TSOs to develop "*requirements on coordination and information exchange between regional security coordinators in relation to the tasks listed in Article 77(3)*".
Article 77, notably its paragraph 3, requires all TSOs of each CCR to delegate to one or more RSCs the following tasks at regional level:

- Regional operational security coordination in accordance with Art 78
- Build of CGM in accordance with Art 79
- Regional outage coordination in accordance with Art 80
- Regional adequacy assessment in accordance with Art 81.

In a meshed system, when a RSC provides its tasks to the TSOs in accordance with Art 77, it can be expected that the issued proposals (and then the decisions once made by TSOs) may have adjacent effects on other TSOs having delegated these tasks to another RSC, while there maybe also additional opportunities for the RSC to provide alternative proposals using remedial actions located within the control areas of these other TSOs.
As a result, RSCs shall provide their tasks with an adequate level of coordination between them. This is explicitly mentioned in each of the SO GL Articles 78 to 81. This implies also requirements on information exchange between the RSCs to support this coordination, leading to an adequate level of interoperability between them. CSAM Chapter 5 provides the corresponding pan-European requirements.
It shall be noted that when developing these requirements, TSOs[7] have taken into account the need for a right balance between

(i) establishing pan-European requirements which provide common sets of rules absolutely needed to ensure the capability for coordination between all RSCs
(ii) leaving enough flexibility for TSOs of each CCR to determine different organisations or execution features (e.g. frequency and conditions of intra-day CGM and regional security analyses updates), depending on the regional characteristics, in accordance with SO GL articles 76 and 77.

The pan-European requirements defined in CSAM cover general needs for inter-RSC coordination and specific needs as regards each of the four tasks.

6.1 General requirements

In order to ensure feasibility of the inter-RSC coordination, CSAM Art 26 requires the use of English for all kind of information exchange between RSCs and requires a 24/7 availability so that any request for coordination coming from one RSC can be addressed by another one. Nevertheless, taking into account that, contrary to TSCNet and Coreso, new RSCs have to be set-up in order to implement SO GL, and consequently have to progressively consolidate their operational organization, Art 26 provides that if a RSC is not able to provide 24/7 availability, a back-up solution shall be defined by the RSC and its TSOs to allow possible exchange of information at the request of other RSCs during the periods this RSC is unavailable.
As mentioned before, RSCs zones of analyse/recommendations cannot be totally independent because of the interconnection of the system (this is true even when the zones are linked by HVDC links). Thus, it is important that the RSCs and their TSOs identify precisely the part of their areas which interact, in order that they specially coordinate their work on these areas. More precisely, to ensure an efficient delivery of the tasks, notably coordinated regional operational security

[7] Indeed, this part of the CSAM has been developed by a working group consisting of TSO and RSC representatives

assessment, each couple of RSCs and their TSOs are required in Art 27 to determine their "overlapping zone", in terms of lists of network elements monitored by each RSC, and list of typical remedial actions used to solve congestions. As regards remedial actions, they have also to identify those which are qualified as "cross-regional" ones. This last notion means that such a remedial action, considered by one RSC to solve a congestion, may have a sufficient impact on a TSO who has delegated its tasks to the other RSC, so that this impacted TSO and its RSC shall be included in the agreement of such a remedial action.

6.2 Requirements linked to CGM build

As the CGM is a fundamental input for the delivery of the 3 other tasks required by SO GL (as well as delivery of capacity calculation task), the highest possible level of availability for the CGMs has to be ensured via a relevant organization set up by the RSCs. It is the objective of Article 29 which aim at organizing RSCs so that they ensure an absence of interruption of the service. Note that this objective is possible, while demanding for all RSCs to implement it, because the "CGM build" task is functionally identical from one region to another one, whereas it would be difficult to set the same requirements for other tasks, as they can be organized differently (e.g. different tools, different timescales, different human expertise role…) and need regional expertise.
CSAM also recognizes that the quality of the IGMs provided by the TSOs is a fundamental pillar in the creation of a consistent CGM, on which other tasks can be delivered with a sufficient accuracy. According to SO GL Art 79(1), each RSC shall check the quality of the IGMs in order to contribute to building the CGM for each mentioned time-frame in accordance with the CGM methodology provisions. In addition, CSAM article 28 requires them to monitor the correct inclusion of all the previously agreed coordinated remedial actions in the IGMs by the TSOs, because the experience shows that any mistake in this inclusion is a risk of confusion and inappropriate diagnosis or decision by the affected TSOs.

6.3 Requirements linked to coordinated regional operational security assessment

The coordinated regional operational security assessment process is performed at RSC level based on a regional methodology defined in the scope of application of Art 76 and 78 of SO GL, and taking into account requirements set-up in CSAM. As a result, these regional methodologies have necessarily some common features such as:

- A list of contingencies that are simulated during the process
- A list of grid elements that are monitored during the process (following CSAM Article 20)
- A list of remedial actions that are used to solve congestions during the process
- Some specific exchange modalities and timestamps during the process to share and agree on the congestions and the Remedial Actions used to solve them.

As a matter of fact, there is a need to properly coordinate these elements at an inter-RSC level to ensure that:

(a) there is no confusion on what is monitored,
(b) the results of the security analyses are shared and they can be cross-checked between RSCs for overlapping zones if needed
(c) the remedial actions proposed and agreed on do not introduce problems at the cross-regional level.

As already mentioned, point (a) is covered by CSAM Article 26. Point (b) is covered by Article 32, requesting to exchange at least the results of security analyses on the overlapping zones and, the need for remedial actions. Point (c) is covered by Article 30 combined with Article 27.

ENTSO-E AISBL • Avenue de Cortenbergh 100 • 1000 Brussels • Belgium • Tel + 32 2 741 09 50 • Fax + 32 2 741 09 51 • info@entsoe.eu • www. entsoe.eu

At the same time, the coordination between RSCs shall aim to allow that the most effective and economically efficient remedial actions, possibly outside the covered area, are found and agreed on during the process. This latter point is particularly relevant when no remedial action can be found by an RSC within the control areas of the TSOs it serves. This cross-regional search of potential remedial action is covered by CSAM Article 31 (but also Article 30(4)), acknowledging that such an investigation can be restricted, in the case of costly remedial actions, to the set of remedial actions which are covered by an existing cost sharing rules agreement between the concerned TSOs.

Besides these requirements developed to ensure general inter-RSC coordination, applicable at any time and triggered by one RSC towards the other ones having overlapping zones with it, CSAM identifies the need for a specific process in Day-ahead to be described. Chapter 2.1 of the supporting document provides more insights on this day-ahead process.

6.4 Requirements linked to outage planning coordination

The Outage Planning is a coordinated process among the participating TSOs and is supported by RSCs in the scope of application of Art 80 "Regional outage coordination". This task requires numerous recurring exchanges of information between TSOs and RSCs. As regions are not independent between them, it is necessary for RSCs to coordinate in order to facilitate identifying possible cross-regional solutions to remove an outage incompatibility for which satisfying solutions have not been found inside a region.
This objective is covered by CSAM Article 35.

6.5 Requirements linked to regional adequacy assessment

The adequacy assessment tasks performed regionally are not independent from each other as the European electricity system can't be split into fully independent regions. This requires timely exchange of information between RSCs before the regional adequacy assessment is performed by RSCs in one region. This exchange of information may also give the opportunity to get and share an overall though not detailed assessment of the risk of adequacy issue at cross-regional level before starting the necessary regional adequacy assessment.

After the regional assessments are performed, some adequacy issues detected regionally that can't be solved into one region could be solved by another adjacent region provided enough energy/MW capacity is available in that region and transmission capacities are available between those regions. Therefore, after the regional assessment is performed, potential cross-regional remedial actions should then be exchanged and assessed between RSCs.
This objective is covered by CSAM Article 36.

7. ENTSO-E role

This part of the supporting document deals with Art 75(1)(e) which requires all TSOs to define the "*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*".

The legal analysis is that providing a direct answer to this requirement rises questions as it is not in the scope of responsibility of the NRAs to decide upon a task given to ENTSO-E. In order to allow TSOs to fulfil their obligation of Art 75(1)(e), while providing a proposal that NRAs can approve, the CSAM requirements are addressed to TSOs, mentioning where useful that TSOs shall use ENTSO-E as a platform for their cooperation to implement the corresponding CSAM requirements.

7.1 Governance

CSAM Article 40 requests TSOs, with the support of the RSCs, to identify the needs for tools and functions of pan-European nature. Such tools should make possible the access and exchange of information between TSOs and/or between RSCs, when such an exchange is needed to prepare secure operation. These tools and functions may be operated in one or several places, by operator(s) such as RSCs, TSOs… Currently, some examples have been identified, e.g. grid model building, OPDE general services to access/retrieve/update/secure data stored in OPDE or alignment of net positions between IGMs.

In the future, extension of these needs or new needs may appear and will have to be conveniently identified and addressed, primarily at pan-European level but it may also concern a need identified at regional level, where the need is shared between several regions and characteristics and processes are common (or largely common) between these regions.

With the variety of the possible needs, it is not meaningful to provide for a unique solution as regards the governance of development and operation of such tools/functions, but it is important to orientate the satisfaction of these needs in an efficient and interoperable way, hence to avoid parallel inconsistent answers provided.

Therefore, for the identified needs, CSAM Article 40 also requires the concerned TSOs to set-up a common development of a tool or a function, i.e. the TSOs shall define how to develop and maintain it, how to finance it, shall define governance rules and agree on the conditions to operate it (e.g. selection of hosting entities).

7.2 Data quality

As regards the data quality issues for operational planning, the fundamental point is to ensure quality of the system modelling. The corresponding requirements are already embedded in CGM methodology (CGMM). This includes an advance process, with the definition of a set of rules and the monitoring of the actual quality, notably with respect to these rules.

Beyond the data quality requirements for CGM building, there is no evidence that other strong data quality requirements need to be identified explicitly, and therefore no evidence that a systematic ENTSOE-role should be determined.

It is the reason why CSAM Article 41 only requires the TSOs, when identifying common needs for functions/tools in accordance with CSAM Art 40, to also identify if those needs would need a specific data quality management process comparable to the one developed in the CGMM, and in that case to define it.

7.3 Monitoring

As regards the end of SO GL Art 75(1)(e), it can be understood that the underlying objective of such a monitoring is to identify the remaining weaknesses, if any, of the regional or pan-European coordination, in order to correct them.

This part of the requirement is worded in a very general form and could be extensively interpreted as a monitoring of all the Articles adopted in the methodology on the five main aspects developed in accordance with SO GL Art 75, together with a monitoring of all the provisions set-up by TSOs and RSCs in each CCR, in accordance with SO GL Art 76. This could lead to a complex and inefficient process of data collection and analysis with poor certainty of being able to identify effective issues/weaknesses.

Moreover, the answer provided to SO GL Art 75(1)(e) requirement shall absolutely avoid becoming redundant with implementation of SO GL Art 17(1), which requests ENTSO-E to report every year on "regional coordination assessment", on the basis of data reported by RSCs, in accordance with SO GL Art 17(2).

As a result, Art 42 CSAM rather opts for a more comprehensive and holistic approach, which consists in requesting all TSOs, using ENTSO-E resources, to make an inquiry towards TSOs and RSCs, every three years, aiming at collecting their diagnosis about the efficiency of the coordination rules applied. This inquiry shall facilitate the establishment of conclusions regarding data quality, efficiency of processes, availability of remedial actions to solve problems in a coordinated way, existing barriers to coordination.

When designing this inquiry, TSOs will have the flexibility to proceed through a qualitative approach versus some quantitative indicators or a mix of both, and will take into account all the information provided by the annual report established in accordance with SO GL Art 17.

ENTSO-E AISBL • Avenue de Cortenbergh 100 • 1000 Brussels • Belgium • Tel + 32 2 741 09 50 • Fax + 32 2 741 09 51 • info@entsoe.eu • www. entsoe.eu

ANNEX I: Cross-reference between SO GL requirements and CSA/RAOC methodologies

As regards the five items required to be addressed in Art 75(1), CSAM provides the following articles:

75(1)(a): Articles 3, 4, 5, 6
75(1)(b): Articles 7, 8, 9, 10, 11, 12, 13, 43
75(1)(c): Articles 22, 23, 24, 25, 37, 38, 39
75(1)(d): Articles 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36
75(1)(e): Articles 40, 41, 42

In addition, CSAM provides requirements for coordination of remedial actions which need to be coordinated by TSOs, with the support of RSCs where applicable, in Articles 14, 15, 16, 17, 18, 19, 20, 21, including aspects to be specified by TSOs in their proposals provided in accordance with SO GL Article 76.

There follows an exhaustive list of references to Art 75 and 84 in SO GL and how they are addressed directly or indirectly in CSAM and RAOCM.

References to Article 75

Article / text	CSA Methodology
23(2).When preparing and activating a remedial action, including redispatching or countertrading pursuant to Articles 25 and 35 of Regulation (EU) 2015/1222, or a procedure of a TSO's system defence plan which affects other TSOs, the relevant TSO shall assess, in coordination with the TSOs concerned, the impact of such remedial action or measure within and outside of its control area, in accordance with Article 75(1), Article 76(1)(b) and Article 78(1), (2) and (4) and shall provide the TSOs concerned with the information about this impact.	CSAM provides requirements for Article 76 methodologies to identify 'cross-border relevant remedial actions', i.e. those requiring coordination, and provides a quantitative influence factor and the associated threshold to be used by default.
33(1) The contingency list shall include both ordinary contingencies and exceptional contingencies identified by application of the methodology developed pursuant to Article 75.	CSAM provides steps for identification of exceptional contingencies associated to a high probability (existence of an occurrence increasing factor) and/or to a high impact (to be defined at TSO level or at inter-TSO level when impact is cross-border).
33(4) Each TSO shall coordinate its contingency analysis in terms of coherent contingency lists at least with the TSOs from its observability area, in accordance with the Article 75.	CSAM provides requirements for TSO to share their contingency list with TSOs whose observability area contains elements of this contingency list. CSAM provides requirement for TSO to include in their contingency list: -external ordinary contingencies -external exceptional contingencies that may endanger their grid.
43(1) Each TSO shall determine the observability area of the transmission-connected distribution systems which is needed for the TSO to determine the system state accurately and efficiently, based on the methodology developed in accordance with Article 75.	CSAM provides steps for identification of observability area both in horizontal (TSO-TSO) and vertical direction (TSO-DSO) direction.
43(2) If a TSO considers that a non-transmission-connected distribution system has a significant influence in terms of voltage, power flows or other electrical parameters for the representation of the transmission system's behaviour, such distribution system shall be defined by the TSO as being part of the observability area in accordance with Article 75.	CSAM provides steps for identification of observability area both in horizontal (TSO-TSO) and vertical direction (TSO-DSO), including the case of non-transmission-connected distribution system.
70(5) Each TSO shall assess the accuracy of the variables in paragraph 3 by comparing the variables with their actual	In the short term, the principle as regards Article 75(1)(c) being to use best forecast estimates in the IGM/CGM, the application of Art 70(5) by any TSO is to compare actual

values, taking into account the principles determined pursuant to Article 75(1)(c).	versus forecasted values and analyse the impact of the differences
72(2) When performing a coordinated operational security analysis, the TSO shall apply the methodology adopted pursuant to Article 75.	CSAM provides requirements concerning: -definition of contingency list -preparation of IGMs and coordinated execution of tasks by TSOs and RSCs -identification of cross-border or cross-regional relevance of remedial actions
75(1) (a) methods for assessing the influence of transmission system elements and 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;	Mathematical method for assessing the influence of transmission system elements and SGUs located outside of a TSO's control area is provided in the Annex I of CSAM and RAOCM
(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;	CSAM provides requirements concerning: 1. Occurrence increasing factors 2. Evolving contingencies affecting one or several TSOs 3. High impact contingencies affecting one or several TSOs CSAM also provides definitions for remedial actions depending on their activation time (preventive, curative, restoring) and requirements for the exchange of information required to establish external contingency lists and for the identification of remedial actions requiring coordination.
(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;	CSAM provides requirements needed at pan-European level to address effects of uncertainties in the long-term and short-term timelines. In the short term, CSAM relies on proven classical approach based on best forecasts and frequency of forecast updates to be determined by TSOs at regional level. This method acknowledges the fact that reliability margins are already taken into account during capacity calculations and thus avoids adding additional not justified margins. See also cross table on Art 75(6).
(d) requirements on coordination and information exchange between regional security coordinators in relation to the tasks listed in Article 77(3);	Articles 26 to 36 provide general requirements aimed at coordination and information exchanges and specific requirements for each task provided by RSCs
(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.	Articles 40 to 41 provide requirements defining how common tools can be identified and governance rules defined by concerned TSOs, and the process to be applied by ENTSOE to monitor the implementation of the CSA methodology and of provisions defined according to Art 76 at regional level.
75 1-2 The methods referred to in point (a) of paragraph 1 shall allow the identification of all elements of a TSO's observability area, being grid elements of other TSOs or transmission-connected DSOs, power generating modules or demand facilities. Those methods shall take into account the following transmission system elements and SGUs' characteristics: (a) connectivity status or electrical values (such as voltages, power flows, rotor angle) which significantly influence the accuracy of the results of the state estimation for the TSO's control area, above common thresholds; (b) connectivity status or electrical values (such as voltages, power flows, rotor angle) which significantly influence the accuracy of the results of the TSO's operational security analysis, above common thresholds; and (c) requirement to ensure an adequate representation of the connected elements in the TSO's observability area. 3. The values referred to in points (a) and (b) of paragraph 2 shall be determined through situations representative of the various conditions which can be expected, characterised by	Mathematical method for assessing the influence of grid elements located outside of a TSO's control area is provided in Annex I of the CSAM.. Furthermore, CSAM provides steps (process) with qualitative/quantitative aspects for identification of observability area both in horizontal (TSO-TSO) and vertical direction (TSO-DSO). In order to tackle different conditions which can be expected CSAM requires TSOs to assess the influence of the elements on different scenarios using CGMSs required by Art. 67 of SO GL. CSAM also requires TSOs to reassess their observability area periodically using qualitative or quantitative approach. TSOs may use dynamic studies (e.g. rotor angle evaluation, but not limited to it) in determination of observability area. Note that for definition of observability area only computation of influence factors of grid elements are necessary. RAOCM provides mathematical method for computation of influence factors of SGUs.

variables such as generation level and pattern, level of electricity exchanges across the borders and asset outages.	
75.4. The methods referred to in point (a) of paragraph 1 shall allow the identification of all elements of a TSO's external contingency list with the following characteristics: (a) each element has an influence factor on electrical values, such as voltages, power flows, rotor angle, in the TSO's control area greater than common contingency influence thresholds, meaning that the outage of this element can significantly influence the results of the TSO's contingency analysis; (b) the choice of the contingency influence thresholds shall minimize the risk that the occurrence of a contingency identified in another TSO's control area and not in the TSO's external contingency list could lead to a TSO's system behaviour deemed not acceptable for any element of its internal contingency list, such as an emergency state; (c) the assessment of such a risk shall be based on situations representative of the various conditions which can be expected, characterised by variables such as generation level and pattern, exchange levels, asset outages.	Mathematical method for assessing the influence of grid elements located outside of a TSO's control area is provided in Annex I of the CSAM. Furthermore, CSAM provides steps (process) with qualitative/quantitative aspects for identification of contingency list.
75.5. The principles for common risk assessment referred to in point (b) of paragraph 1 shall set out criteria for the assessment of interconnected system security. Those criteria shall be established with reference to a harmonised level of maximum accepted risk between the different TSO's security analysis. Those principles shall refer to: (a) the consistency in the definition of exceptional contingencies; (b) the evaluation of the probability and impact of exceptional contingencies; and (c) the consideration of exceptional contingencies in a TSO's contingency list when their probability exceeds a common threshold.	CSAM provides requirements concerning 1. Common definition of types of exceptional contingencies 2. Common definition of occurrence increasing factors 3. The inclusion of an exceptional contingency in the contingency list as soon as one occurrence increasing factor is higher than the associated application criteria.
75.6. The principles for assessing and dealing with uncertainties referred to in point (c) of paragraph 1 shall provide for keeping the impact of the uncertainties regarding generation or demand below an acceptable and harmonised maximum level for each TSO's operational security analysis. Those principles shall set out: (a) harmonised conditions where one TSO shall update its operational security analysis. The conditions shall take into account relevant aspects such as the time horizon of the generation and demand forecasts, the level of change of forecasted values within the TSO's control area or within the control area of other TSOs, location of generation and demand, the previous results of its operational security analysis; and (b) minimum frequency of generation and demand forecast updates, depending on their variability and the installed capacity of non-dispatchable generation.	In long term, CSAM basis for uncertainties management is the possibility for TSOs to add local scenarios to the common scenarios defined pursuant to SO GL Art 65. In the short-term, CSAM Art 24 requires TSOs to identify the frequency of intraday security analyses required by their local conditions, which cover the aspects required by Art 75(6). This is complemented by the fact that TSOs at regional level have to define needed frequency of regional security assessments by RSCs, according to Art 76. CSAM Art 37-38 defines the frequency of load and RES forecast updates, depending of the level of their impact on the control area.
76(1) …The proposal shall respect the methodologies for coordinating operational security analysis developed in accordance with Article 75(1)	The CSAM provides the common requirements to be applied at pan-European level which are deemed necessary to ensure the global security of the interconnected system while leaving flexibility to design appropriately the TSOs proposal for regional delivery of the four tasks required by SO GL requested by Art 76-77
78(1)(a) Each TSO shall provide the regional security coordinator with all the information and data required to perform the coordinated regional operational security assessment, including at least: (a) the updated contingency list, established according to the criteria defined in the methodology for coordinating operational security analysis adopted in accordance with Article 75(1);	CSAM Article 11 defines how a TSO shall inform other TSOs and relevant RSCs of any change in its exceptional contingency list.

References to Article 84

84 2.The methodology referred to in paragraph 1 shall be based on qualitative and quantitative aspects that identify the impact on a TSO's control area of the availability status of either power generating modules, demand facilities, or grid elements which are located in a transmission system or in a distribution system including a closed distribution system, and which are connected directly or indirectly to another TSO's control area and in particular on: (a) quantitative aspects based on the evaluation of changes of electrical values such as voltages, power flows, rotor angle on at least one grid element of a TSO's control area, due to the change of availability status of a potential relevant asset located in another control area. That evaluation shall take place on the basis of year-ahead common grid models; (b) thresholds on the sensitivity of the electrical values referred to in point (a), against which to assess the relevance of an asset. Those thresholds shall be harmonised at least per synchronous area; (c) capacity of potential relevant power generating modules or demand facilities to qualify as SGUs; (d) qualitative aspects such as, but not limited to, the size and proximity to the borders of a control area of potential relevant power generating modules, demand facilities or grid elements; (e) systematic relevance of all grid elements located in a transmission system or in a distribution system which connect different control areas; and (f) systematic relevance of all critical network elements. 3.The methodology developed pursuant to paragraph 1 shall be consistent with the methods for assessing the influence of transmission system elements and SGUs located outside of a TSO's control area established in accordance with Article 75(1)(a).	RAOCM provides steps for identification of Relevant Assets. Mathematical method for assessing the influence of transmission system elements and SGUs located outside of a TSO's control area is provided in Annex I of the RAOCM. Furthermore, RAOCM provides steps (process) with qualitative/quantitative aspects for identification of elements, which a TSO considers relevant for outage coordination. Furthermore, RAOCM provides process for TSOs of each CCR how to determine Relevant Assets list and defines requirements concerning updates of Relevant Assets List. TSOs may use dynamic studies (e.g. rotor angle evaluation, but not limited to it) in determination of relevant assets.
85.1 By 3 months after the approval of the methodology for assessing the relevance of assets for outage coordination in Article 84(1), all TSOs of each outage coordination region shall jointly assess the relevance of power generating modules and demand facilities for outage coordination on the basis of this methodology, and establish a single list, for each outage coordination region, of relevant power generating modules and relevant demand facilities	RAOCM provides process for TSOs of each CCR how to determine Relevant Assets list. Furthermore, RAOCM also provides requirements concerning updates of Relevant Assets List.
86.1 Before 1 July of each calendar year, all TSOs of each outage coordination region shall jointly re-assess the relevance of power generating modules and demand facilities for outage coordination on the basis of the methodology developed in accordance with Article 84(1). 2. Where necessary, all TSOs of each outage coordination region shall jointly decide to update the list of relevant power generating modules and relevant demand facilities of that outage coordination region before 1 August of each calendar year.	RAOCM provides process for TSOs of each CCR how to determine Relevant Assets list. Furthermore, RAOCM also provides requirements concerning updates of Relevant Assets List.
87 1. By 3 months after the approval of the methodology for assessing the relevance of assets for outage coordination in Article 84(1), all TSOs of each outage coordination region shall jointly assess, on the basis of this methodology, the relevance for the outage coordination of grid elements located in a transmission system or in a distribution system including a closed distribution system and shall establish a single list, per outage coordination region, of relevant grid elements. 2. The list of relevant grid elements of an outage	RAOCM provides process for TSOs of each CCR how to determine Relevant Assets list. Furthermore, RAOCM also provides requirements concerning updates of Relevant Assets List.

coordination region shall contain all grid elements of a transmission system or a distribution system, including a closed distribution system located in that outage coordination region, which are identified as relevant by application of the methodology established pursuant to Article 84(1).	
88.1 Before 1 July of each calendar year, all TSOs of each outage coordination region shall jointly re-assess, on the basis of the methodology established pursuant to Article 84(1), the relevance for the outage coordination of grid elements located in a transmission system or a distribution system including a closed distribution system. 2. Where necessary, all TSOs of an outage coordination region shall jointly decide to update the list of relevant grid elements of that outage coordination region before 1 August of each calendar year.	RAOCM provides process for TSOs of each CCR how to determine Relevant Assets list. Furthermore, CSAM also provides requirements concerning updates of Relevant Assets List.

ANNEX II: Effect of generation pattern/level of flows on the calculation of influence factors

This ANNEX provides an explanation why the generation pattern and level of flows in the respective scenarios have a negligible effect on the influence factors calculated in accordance with CSAM and RAOCM. For that, a method based on DC load flow computation is shown that can be used to compute such influence factors.

The first step of computing influence factors with the aforementioned method is calculation of so-called I*njection Shift Factors (ISFs)*. These enable the calculation of the corresponding P*ower Transfer Distribution Factors (PTDFs)* which again enable the calculation of *Line Outage Distribution Factors (LODFs)*. These LODFs show how the flow on one line distributes among other lines in case of an outage of the line. They are identical to the corresponding influence factors calculated in accordance with CSAM and RAOCM.

ISFs, PTDFs and LODFs are commonly used in tasks linked to power flow computation. More information can be found in the technical and scientific literature.

Computation method

For an arbitrary grid with N_n nodes and N_b branches, the incidence matrix and the diagonal branch susceptance matrix are built. The incidence matrix $\boldsymbol{A}$ is a $N_b \times N_n$ matrix. If a branch b starts in node n, the formula $\boldsymbol{A}(b,n) = 1$ applies. If branch b ends in node n, the formula $\boldsymbol{A}(b,n) =$ -1 applies. The formula $\boldsymbol{A}(b,n) = 0$ applies in all other cases. The diagonal branch susceptance matrix is a $N_b \times N_b$ diagonal matrix. The formula $\boldsymbol{B}(b,b) = \frac{1}{X_b}$ is applied here. For simplification, a $N_b \times N_n$ matrix $\breve{\boldsymbol{B}} = \boldsymbol{B} \cdot \boldsymbol{A}$ is defined. Using these matrices, the $N_n \times N_n$ susceptance matrix $\widetilde{\boldsymbol{B}}$ of the grid is determined according to (F.1).

$$\widetilde{\boldsymbol{B}} = \boldsymbol{A}^T \cdot \boldsymbol{B} \cdot \boldsymbol{A} = \boldsymbol{A}^T \cdot \breve{\boldsymbol{B}} \qquad \text{(F.1)}$$

This matrix is needed to determine the $N_b \times N_n$ ISF matrix using 2). The ISF matrix is only valid for an arbitrary fixed slack node and an arbitrary reference node. The values of the ISF matrix depend on the chosen slack node while the chosen reference node has no effect on the matrix.

$$\boldsymbol{ISF} \cdot \boldsymbol{T}_{\neg slack} = \breve{\boldsymbol{B}} \cdot \boldsymbol{T}_{\neg ref} \cdot \left(\boldsymbol{T}_{\neg slack}^{T} \cdot \widetilde{\boldsymbol{B}} \cdot \boldsymbol{T}_{\neg ref}\right)^{-1} \qquad \text{(F.2)}$$

The matrices $\boldsymbol{T}_{\neg slack}$ and $\boldsymbol{T}_{\neg ref}$ are transformation matrices that remove the column of the slack node and the reference node respectively. They are equal to identity matrices with the respective columns removed. When transposed, they remove the corresponding rows using a left multiplication.

When injecting power in node n and extracting it from the slack node, the matrix element $\boldsymbol{ISF}(b,n)$ shows the fraction of the injected power by which the load flow on branch b changes. In the ISF matrix, the column of the slack node, which cannot be determined using formula 2), is filled with zeros. This is obvious as injecting power in the slack node and extracting the same power from it has no effect on any branches of the grid. Given that information, the whole ISF matrix is known.

The ISF matrix depends only on the topology of the grid and is independent of the production pattern. However, although this is not needed for influence factor computation, the ISF matrix could be used to compute the load flows resulting from a particular production pattern by multiplying the ISF matrix with the corresponding matrix of all injections and withdrawals.

To continue the computation of influence factors, using the previously calculated ISF matrix and formula (F.3), the $N_b \times N_b$ PTDF matrix of the grid can be calculated.

$$\boldsymbol{PTDF} = \boldsymbol{ISF} \cdot \boldsymbol{A}^T \tag{F.3}$$

This multiplication is shown in (F.4) for one matrix element.

$$\boldsymbol{PTDF}(t,r) = \boldsymbol{ISF}\left(t,n_{r,s}\right) - \boldsymbol{ISF}\left(t,n_{r,e}\right) \tag{F.4}$$

In that formula, t and r can be any branches of the grid. The indices $n_{r,s}$ and $n_{r,e}$ are the nodes in which branch r starts and ends respectively. In (F.3) they result from the incidence matrix. Looking at (F.4), the meaning of a matrix element $\boldsymbol{PTDF}(t,r)$ becomes obvious. When injecting power in the start node of branch r and extracting it in the end node of branch r, the matrix element $\boldsymbol{PTDF}(t,r)$ shows the fraction of the injected power by which the load flow on branch t changes. As two ISFs are substracted, the influence of the slack node is removed. The PTDF matrix is thus independent of the slack node chosen in the previous step.

To finalize the computation of influence factors, the LODFs need to be calculated. This is done by using the previously determined PTDF matrix and (F.5).

$$\boldsymbol{LODF}(t,r) = \frac{\boldsymbol{PTDF}(t,r)}{1 - \boldsymbol{PTDF}(r,r)}, \qquad t \neq r \tag{F.5}$$

The LODFs show how the flow on a branch distributes among other branches in case of tripping. For tripping of a branch r, the matrix element $\boldsymbol{LODF}(t,r)$ shows the change of flow on branch t as a fraction of the flow on branch r before tripping. The values of the diagonal elements of the LODF matrix cannot be calculated using (F.5). These values are obviously -1, as the flow on an element changes to zero when tripping.

$$\boldsymbol{LODF}(r,r) = -1 \tag{F.6}$$

Link to formulae in CSAM and RAOCM

In the annexes of CSAM and RAOCM, the following formulae are used:

$$IF_r^{pf,id} = MAX_{\forall i \epsilon I, \forall s, \forall t \epsilon T}\left(\frac{P_{s,n-i-r}^t - P_{s,n-i}^t}{P_{s,n-i}^r} \cdot \frac{PATL^{s,r}}{PATL^{s,t}} \cdot 100\%\right) \tag{F.7}$$

$$IF_r^{pf,f} = MAX_{\forall i \epsilon I, \forall s, \forall t \epsilon T}\left(\frac{P_{s,n-i-r}^t - P_{s,n-i}^t}{P_{s,n-i}^r} \cdot 100\%\right) \tag{F.8}$$

In these formulae, the respective LODF matrix elements $\boldsymbol{LODF}_{s,\neg i}(r,r)$ can be inserted with s depicting the scenario used and $\neg i$ indicating that the element i is removed from the network provided in the scenario. This leads to:

$$IF_r^{pf,id} = MAX_{\forall i \epsilon I, \forall s, \forall t \epsilon T}\left(\boldsymbol{LODF}_{s,\neg i}(t,r) \cdot \frac{PATL^{s,r}}{PATL^{s,t}} \cdot 100\%\right) \tag{F.9}$$

and (F.10)

$$IF_r^{pf,f} = MAX_{\forall i \epsilon I, \forall s, \forall t \epsilon T}\left(\boldsymbol{LODF}_{s,\neg i}(t,r) \cdot 100\%\right)$$

Conclusion

As all factors in formulae (F.9) and (F.10) are independent of generation patterns and the level of load flows, it must be concluded that the influence factors do not depend on them as well. Indeed it is shown that they only depend on the grid topologies provided in the scenarios, including the PATLs in case of $IF_r^{pf,id}$. The removal of an element i also affects the topology only.

As the example shows, the influence factors are absolutely independent of generation patterns and the level of load flows when using a DC load flow based approach to compute the influence factors.

It should not be concealed that generally there can be effects of the level of load flows and generation patterns when using AC load flow based approaches to compute influence factors. However, as differences in results of AC and DC based load flow computation are limited, it can easily be concluded that the effects on influence factors are small when using an approach based an AC load flow computation. This has also been verified by exhaustive computations executed in the course of developing CSAM and RAOCM.