SUPPORTING PAPER FOR THE OPERATIONAL SECURITY NETWORK CODE

14.12.2012

RESULTS OF PUBLIC CONSULTATION:

1 PURPOSE AND OBJECTIVES OF THIS DOCUMENT 4
1.1 PURPOSE OF THE DOCUMENT 4
1.2 STRUCTURE OF THE DOCUMENT 4
1.3 LEGAL STATUS OF THE DOCUMENT 4
2 PROCEDURAL ASPECTS 4
2.1 INTRODUCTION 4
2.2 THE FRAMEWORK FOR DEVELOPING NETWORK CODES 5
3 SCOPE, STRUCTURE & APPROACH TO DRAFTING THE OS NC 6
3.1 BACKGROUND 6
3.2 GUIDING PRINCIPLES 6
3.3 STRUCTURE 7
3.4 LEVEL OF DETAIL 7
3.5 CHALLENGES AND OPPORTUNITIES AHEAD FOR SYSTEM OPERATION 8
3.5.1 Challenges for System Operation 8
3.5.2 Risks and Opportunities 9
3.6 INTERACTION WITH OTHER NETWORK CODES 11
3.7 WORKING WITH STAKEHOLDERS& INVOLVED PARTIES 14
4 RELATIONSHIP BETWEEN THE OS NC & FRAMEWORK GUIDELINES 15
5 PROVISIONS OF THE OS NC 17
5.1 SYSTEM STATES 17
5.2 FREQUENCY CONTROL MANAGEMENT 18
5.3 VOLTAGE CONTROL AND REACTIVE POWER MANAGEMENT 18
5.4 SHORT-CIRCUIT CURRENT MANAGEMENT 19
5.5 POWER FLOWS MANAGEMENT 19
5.6 CONTINGENCY ANALYSIS AND HANDLING 19
5.7 PROTECTION 21
5.8 DYNAMIC STABILITY MANAGEMENT 21
5.9 OPERATIONAL TRAINING AND CERTIFICATION 21
6 NECESSARY DATA AND INFORMATION FOR SAFEGUARDING THE OPERATIONAL SYSTEM SECURITY 23
6.1 INTRODUCTION 23
6.2 TASKS OF THE TRANSMISSION SYSTEM OPERATORS 24
6.3 THE OS NC AS A PLACEHOLDER OF THE TOPIC DATA EXCHANGE FOR OPERATIONAL PURPOSE 25
6.4 THE TWO WAYS OF EXCHANGING DATA WITH THE TSO SET BY THE OS NC 26
7 COMPLIANCE, TESTING AND INVESTIGATION IN THE FRAMEWORK OF THE OS NC 26
7.1 COMMON TESTING AND INCIDENT ANALYSIS RESPONSIBILITIES 26
7.1.1 The goal of Operational Testing and Monitoring 26
7.1.2 Common Testing and Incident Analysis Responsibilities in the framework of the OS NC 27
7.2 THE INCIDENTS CLASSIFICATION SCALE 27
8 FUNDAMENTAL CONCEPTS & PROCESSES OF THE OS NC 29
8.1 COMMON GRID MODEL (CGM) 29
8.2 SIGNIFICANT GRID USER (SGU) 31
8.3 LFC AREA, RESPONSIBILITY AREA, OBSERVABILITY AREA, ... 32
8.4 N-1 PRINCIPLE 33
8.4.1 (N-1)-assessment: classification of contingencies as a function of probability of occurrence 33

8.5 System States ... 34
8.5.1 Common Awareness System ... 34

9 Added values of the OS NC ... 36

10 Summary of changes to the draft network code ... 38

10.1 Introduction ... 38
10.2 Summary of comments ... 38
10.3 Structural changes in light of comments ... 39
10.4 Enhancing consistency ... 39
10.5 Most Significant Content Related Changes to the Network Code ... 40
10.6 Conclusion ... 40

11 Next Steps ... 40

11.1 Submission to ACER ... 41
11.2 The ACER opinion ... 41
11.3 The Comitology Procedure ... 41
11.4 ENTSO-E steps during this period ... 41
11.5 Entry into Force ... 42

12 References ... 42

Annex 1-Definitions in the framework of the OS NC ... 43

1 PURPOSE AND OBJECTIVES OF THIS DOCUMENT

1.1 PURPOSE OF THE DOCUMENT

This document has been developed by the European Network of Transmission System Operators for Electricity (ENTSO-E) to accompany the Operational Security Network Code (OS NC) and should be read in conjunction with that document.

It aims to provide interested parties with information about the rationale for the approach set out in the OS NC, outlining the reasons that led to the requirements specified in it. The document has been developed in recognition of the fact that the OS NC, which will become a legally binding document after Comitology, inevitably cannot provide the level of detailed explanation which some parties may desire.

1.2 STRUCTURE OF THE DOCUMENT

This document is structured as follows:

- Section 2 introduces the legal framework within which the OS NC has been developed.
- Section 3 explains the approach which ENTSO-E has taken to develop the OS NC, outlining the challenges and opportunities ahead for System Operation.
- Section 4 describes how this Network Code complies with the requirements of the Framework Guidelines on System Operation (SO FG) developed by the Agency for the Cooperation of Energy Regulators (ACER).
- Section 5 focuses on the Requirements of the OS NC by topic.
- Section 6 focuses on the topic Necessary Data and Information for Safeguarding the Operational System Security
- Section 7 handles with the topic Compliance, Testing and Investigation in the framework of the OS NC
- Section 8 presents the fundamental concepts of the OS NC
- Section 9 presents the added values of implementing the operational principles set by the OS NC.
- Section 10 includes a summary of changes to the draft Network Code
- Section 11 summarises the next steps.

Besides, following Annex can be found attached to the OS NC Supporting Document:

- Annex 1 contains the Definitions in the framework of the OS NC.

1.3 LEGAL STATUS OF THE DOCUMENT

This document accompanies the OS NC and is provided for information purposes. Consequently, this document has no legally binding status.

2 PROCEDURAL ASPECTS

2.1 INTRODUCTION

This section provides an overview of the procedural aspects of Network Codesô development. It explains the legal framework within which network codes are developed and focuses on ENTSO-Eõs legally defined roles and responsibilities. It also explains the next steps in the process of developing the OS NC.

2.2 THE FRAMEWORK FOR DEVELOPING NETWORK CODES

This OS NC has been developed in accordance with the process established within the Third Package, in particular in Regulation (EC) 714/2009. The Third Package establishes ENTSO-E and ACER and gives them clear obligations in developing network codes. This is shown in Figure1.

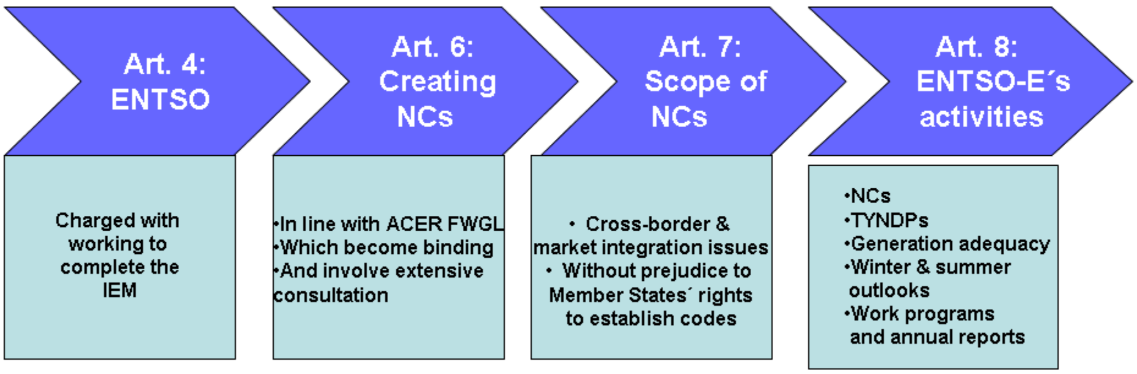

Figure 1: ENTSO-E‘s legal role in network code development according to Regulation (EC) 714/ 2009.

Moreover, this framework defines the process for developing network codes involving ACER, ENTSO-E and the European Commission, as shown in Figure 2:

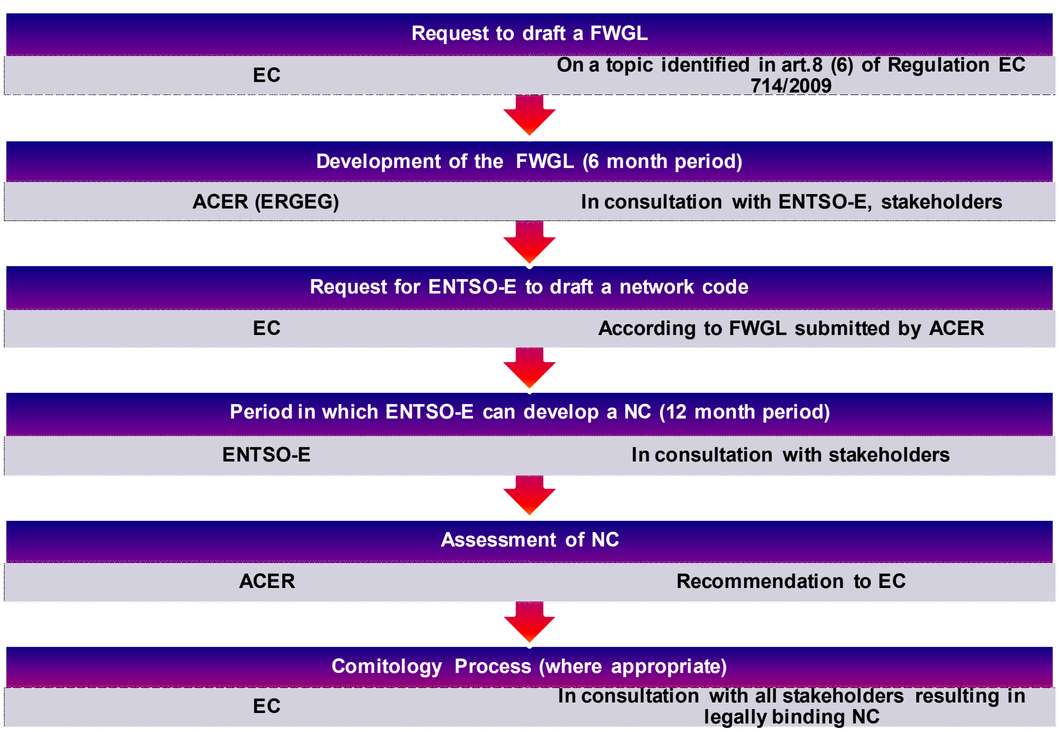

Figure 2: Network Codes' development process *(Source: ENTSO-E).*

The OS NC has been developed by ENTSO-E to meet the requirements of the SO FG [1] published by ACER in December 2011. ACER has also conducted an Initial Impact Assessment associated with its consultation on its draft FG SO in June 2011 [2].

ENTSO-E was formally requested by European Commission to begin the development of the OS NC on 1^{st}March 2012. The deadline for the delivery of the Network Code to ACER is the 1^{st} March 2013.

3 SCOPE, STRUCTURE & APPROACH TO DRAFTING THE OS NC

3.1 BACKGROUND

ENTSO-E has drafted the OS NC to set out clear and objective minimum requirements for real-time Operational Security and achieving the main goal of keeping the European interconnected Transmission Systems in continuous operation, in order to contribute to a harmonised framework for completion of the EU Internal Electricity Market (IEM) and to ensure non-discrimination, effective competition and the efficient functioning of the IEM.

Based on the SO FG and on the Initial Impact Assessment provided by ACER, the OS NC states the Operational Security principles in terms of technical needs, considering market solutions compatible with and supporting security of supply.

3.2 GUIDING PRINCIPLES

The guiding principles of the OS NC are to determine common Operational Security requirements and principles, to ensure the conditions for maintaining Operational Security throughout the EU, to promote for coordination of system operation. These Operational Security principles are essential for the TSOs to manage their responsibilities for operating the interconnected Transmission Systems with a high level of coordination, reliability, quality and stability.

A key goal of the OS NC is to achieve a harmonised and solid technical framework - including the implementation of all necessary processes required for Operational Security, taking into account the rapid growth of Renewable Energy Sources (RES) generation and their impact on System Operation. Consequently, the requirements have been designed in order to ensure secure System Operation, taking into account the integration of RES and the effective development of the IEM.

The requirements set out in OS NC on TSOs, DSOs and Grid Users are building upon a long history of existing common and best practices, lessons learned and operational needs throughout the European Transmission Systems. This, together with the fact that the European experience of interconnected Transmission Systems operation dates back to the 1950-ies (Union for Coordination of (Production) and Transmission of Electricity (UC (P) TE)), 1960-ies (Nordel), and 1970-ies (TSO Associations of Great Britain and Republic of Ireland, UKTSOA and ITSOA), distinguishes the OS NC and all other System Operation Network Codes (SO NCs) from other Network Codes in the following terms:

- The work on the SO NCs has not started from ñscratchò but builds upon a wide and deep range of requirements, policies and standards of the previous European transmission system organisations, adapting and further developing these requirements in order to satisfy the requirements of the SO FG, to meet the challenges of transformations in the energy sector including RES and increasing volatility and dynamics of market operations and to support effective and efficient completion of the IEM.

- The subject matter ï Operational Security of the interconnected Transmission Systems of Europe ï is vital not just for the continuous and secure supply of European citizens with electricity but also for the electricity market to function at all; therefore, any changes, adjustments and developments based on the new (legally binding after Comitology) SO NCôs framework must acknowledge and respect the fact that System Operation cannot be interrupted and ñrestartedò ï we are working on a ñliving gridò.

- By their nature and because of the level of technical detail involving all aspects of Transmission System operations, the SO NCs are mainly addressing the TSOs and ENTSO-E; nevertheless, links and cross-references, as well as practical dependencies and explanations are established in relation to other NCs, most notably those addressing grid connection, market and balancing / regulating power.

3.3 STRUCTURE

Ensuring Operational Security, reliability and quality implies providing a common Security Level within the interconnected Transmission Systems of Europe, requiring the close cooperation of TSOs, DSOs, Generating Facilities and Demand Facilities.

In order to set out clear and objective requirements, the following categories of requirements have been established in the OS NC:

- System states
- Frequency control management
- Voltage control and reactive power management
- Short-circuit current management
- Congestion and power flows management
- Contingency analysis and handling
- Protection
- Dynamic stability management
- Data Exchange
- Operational training and certification
- Common testing and incident analysis responsibilities

3.4 LEVEL OF DETAIL

In order to achieve the necessary level of European harmonisation, allowing at the same time more detailed provisions at the regional/national level where necessary, and with the view of drafting an OS NC open for future developments and new applications, an approach focusing on a pan-European view and the most widely applicable Operational Security requirements has been pursued throughout the development of the OS NC. The SO FG[1] provided further clarification concerning the issue of European-wide applicability, while pointing out that *"… ENTSO-E shall, where possible, ensure that the rules are sufficiently generic to facilitate incremental innovation in technologies and approaches to system operation being covered without requiring code amendments"*.

Thus, the requirements have been drafted considering a period of approximately 5 years as a reasonable cycle within which changes to the OS NC will have to be implemented, building up a coherent legal mechanism with the appropriate balance between level of detail and flexibility.

Whereas this first OS NC picks up as much input from involved parties as possible in order to enable a high level of system security, regional requirements concerning the different Synchronous Areas, regions or even single TSOs may lead to further and more detailed provisions. In any case, compatibility and coherence must be ensured for all provisions defined at the level of Synchronous Area, region or a single TSO.

3.5 Challenges and Opportunities ahead for System Operation

Nowadays, in line with the challenging objectives set out in the SO FG, System Operation goes beyond just operating the electric power system in a safe, secure, effective and efficient manner. Aspects such as enabling the integration of innovative technologies and making use of information and communication technologies must be fully integrated, while applying the same principles for the different Transmission Systems of Europe.

3.5.1 Challenges for System Operation

In this context, the future challenges for System Operation, which are addressed in particular, include:

- Effects resulting from the fast growth of intermittent generation from RES.
- Needs resulting from the evolution (and completion) of the IEM.

Generation from RES

The transmission tasks and challenges within the Transmission Systems of the European TSOs are ever more driven and influenced by the effects of the growing generation from RES. RES generation predominately varies with weather conditions. The characteristic of variability and also uncertainty of RES generation, being difficult to forecast accurately, until close to real time, causes the following consequences for System Operation:

- Renewable energy increasingly replaces the feed-in from large power plants directly connected to the Transmission System;
- During the past several years RES generation has contributed significantly to the increase in and volatility of planned and unplanned cross-border power flows, therefore posing new challenges to maintaining the required balance between production and consumption, and to the management of physical flows over the borders;

---

[1]Article 1.5 Application, Framework Guidelines on System Operation, ACER, December 2011.

- The influence of underlying production leads to a high forecast complexity for the balance of transfers into the Distribution Network and thus also for the prediction of load flows in the Transmission System.

This leads to concerns about how to maintain stable System Operation in an electricity network with high penetration of RES. The general answer to this is to increase the controllability and the flexibility of all elements of the Transmission System. This can in turn lead to a Transmission System which can react and cope better with the intermittency of RES.

Internal Electricity Market (IEM)

Cross border trades and intraday markets have significantly increased in recent years, with the corresponding introduction of intraday capacity allocation and the resulting short-term adjustments to the generating capacity of power plants. Due to this fact and in order to comply with the obligations under Regulation (EC) 714/2009, a short-term update of generation forecasts has become indispensable and reliable System Operation can only be established on the basis of reliable input values.

In addition to the consequences for power flows, large changes on generation programs with different ramp rates (especially non-synchronous ramps) lead to temporary imbalances and can create a frequency deviation; this phenomenon is observed throughout ENTSO-E Regional Group Continental Europe (former UCTE), with an increasing trend in the number, duration, and the amplitudes of these frequency deviations, especially during the ramping periods in the morning and in the evening[2]. Another observed reason for longer periods with large frequency deviations is the persistent imbalance in one or more LFC Areas which cannot be restored due to insufficient secondary (Frequency Restoration Reserve) and/or tertiary (Replacement Reserve) control reserve (in these cases the LFC Areas concerned experience a large ACE (Area Control Error) or an equivalent parameter).

These frequency deviations activate a significant share of the primary control reserve (Frequency Containment Reserve) in the system, which is intended and dimensioned for coping with predictable (in terms of quantity and risk) sudden generation or load outages. Consequently these frequency deviations endanger secure System Operation by depleting the required containment reserves for significant periods.

Another factor has accentuated these frequency deviations: the rapid growth in generation from RES, where the generators used (mainly asynchronous by technology) provide no natural inertia, for frequency response, to the system, compared to the conventional synchronous generators used in the traditional power plants.

3.5.2 Risks and Opportunities

In view of achieving the integration of RES in the system and implementation of the IEM, the following opportunities and challenges (with their associated risks) have been identified as relevant for System Operation. These changes create a scenario with increasing complexity, where further challenges can be foreseen in the near future due to the new applications and developments on system operation, such as:

---

[2] "Deterministic frequency deviations – root causes and proposals for potential solutions", a joint EURELECTRIC – ENTSO-E response paper (https://www.entsoe.eu/news/announcements/newssingleview/article/the-report-on-deterministic-frequency-deviations-root-causes-and-proposals-for-potential-solu/)

- High Voltage DC (HVDC) Links
- Demand Side Response (DSR)
- Smart Grids
- Super Grids

HVDC Links

The operation of HVDC links has to be ensured by TSOs. This requires a systematic approach to their reliability when connected to the continental European AC grid and the consideration of the effects of connecting such large amounts of bi-directional power, in-feed/out-feed to single points, on the operation of the pan-European Transmission System. In addition, the operational impacts of HVDC also need to be accounted for, with their filter banks, zero fault level in-feed and very fast ramping rates.

The common features of devices such as PST (Phase-Shifting Transformers) or FACTS (Flexible Alternating Current Transmission Systems) are their controllability and the large impact they can have on cross-border power flows, including in conjunction with HVDC.

Nevertheless, these also provide opportunities for TSOs to optimise flows and voltages and have to be considered as such. It follows that TSOs have to coordinate the application and operation of PSTs and HVDC lines for coherent and coordinated power flowsôcontrol.

Demand Side Response

Demand Side Response is already becoming a reality, increasing the complexity of system operation due to its corrective control approach. Technical requirements, information provision and co-ordination are therefore needed in order to facilitate DSR resources to support transmission system security and to give demand users access to markets for ancillary services acquired by TSOs.

Smart Grids

Whereas Smart Grids will provide a competitive edge for the IEM, focusing particularly on the Distribution Grids, leading to new products, processes and services. At the same time they will require a transformation of the functionality of the current Transmission and Distribution Systems to achieve the energy policy targets and to guarantee high security, quality and economic efficiency of electricity supply. Moreover, new developments related to aspects such as communication, especially between DSOs and TSOs, IT-infrastructure and new power system applications must be foreseen.

Super Grids

Contrary to the Smart Grids, the term Super Grids stands for the developments almost exclusively affecting the TSOs and Transmission Systems. Whereas the first ideas on a pan-European Super Grid date back to the early 1950-ies, the real needs (i.e. ñcollectingò and delivering wind power from the North and solar power from the South, while fostering evolution of the IEM at the same time) emerge only with the current evolution of the power systems, as a consequence of the energy turnaround. While initially perceived as a future prospect, Super Grids ï building upon additional and substantial AC-lines re-enforcements, as well as greater integration of HV DC technology ï are already becoming a reality today.

The OS NC provisions must therefore also account for the relevant aspects of the Super Grids, which are additionally determining the System Operation and Operational Security of the European Transmission Systems:

- Establishment and usage of the Common Grid Models for all phases of operational planning and real-time System Operation;
- Exchange and coordination of all relevant information and data, both between the TSOs and also between the TSOs and DSOs / System Users. This is an issue which is addressed in detail in Chapter 4 of the OS NC;
- Ensuring the provisions and a firm basis for coordinated control actions of all relevant TSOs , DSOs and System Users, in order to maintain the global and overall view, while at the same time acting locally or regionally to achieve the most efficient and effective results ï maintaining Operational Security and maximizing the welfare from well utilised Transmission System capacities.

Taking into consideration the new developments described in this section and the associated opportunities and challenges for System Operation, the OS NC principles set the base for operational rules and for a technical-operational coordination between TSOs, DSOs and Grid Users in order to deal with issues such as the intermittent generation, with low predictability until closer to real-time, the massive growth of cross-border trade and transits, generation allocation close to real-time and continuously changing or high forecast complexities.

3.6 INTERACTION WITH OTHER NETWORK CODES

The Network Codes Development Process carried out by ENTSO-E addresses the interaction during drafting of several network codes in parallel. That these codes are at the same time both interfacing and influencing each other is a significant issue. While recognising this issue in the early drafting phases of the OS NC, internal coordination has been held between the convenors and drafting teams (regular conveners meetings, workshops between different drafting teams, etc.) to treat the key cross-issues and therefore reach the required close cooperation between the different network codes drafts.

The major cross-issues have been dealt among the different network codes in the following way:

- The Network Codes on *System Operation* - The OS NC can be viewed as the óumbrellaô code for all the System Operation Network Codes. It therefore sets the overall principles for System Operation and reflects on the common high level issues for the Network Codes for Load-Frequency Control and Reserves (LFCR NC), and for Operational Planning and Scheduling (OPS NC). The LFCR NC and OPS NC will describe their specific processes in greater detail. Moreover, issues to be covered in the future Emergency Network Code are referred to where necessary.
- The Network Code on *Capacity Calculation and Congestion Management* (CACM NC) ï was developed in advance of the OS NC, enabling the interfaces between the capacity calculation process and system operation to be identified in the early drafting phase of this code.

  The common work between the Capacity Calculation Drafting Team and the Operational Security Drafting Team led to the classification of topics treated among both codes based on the following reasoning: while topics related to the physical operation of the power system - where physical scenarios are hypothesised and physical risks are involved - are covered by the System Operation Network Codes, topics related to the operation of the electricity market -

where market scenarios are hypothesised and financial risks are involved - are covered by the CACM NC, taking into account the physical risks described in the System Operation Network Codes.

A data list containing the information required as an input for building and implementing a Common Grid Model (CGM) has been shared among the CACM NC, the OS NC and the OPS NC for the following reason: while the Common Grid Model is to be used for capacity calculation, it shares the same technical data that TSOs require for the calculation of load-flows in order to carry out network Security Analysis, taking into account the fulfilment of the (N-1)-criterion.

Furthermore, in order to ensure the appropriate coherency and compatibility and to reach an agreement on the legal approach of the different Network Codes, an internal ENTSO-E Workshop on Capacity Calculation and System Operation Network Codes was organised in December 2011.

- The Grid Connection Codes: *Network Code on Requirements for Grid Connection Applicable for All Generating Facilities (RfG NC) and the Demand Connection Code DCC NC)*

Transmission System Operators are responsible for defining operational practices and operational requirements for Grid users, in order to make the best use of the available infrastructure and to reach European energy policy targets. It is a common practice for TSOs to review these operating practices periodically even if fundamental changes are not frequent. Operating practices have to be adapted to the system evolution, with the load and the generation mix (type and location of generating units) as major drivers, but must at the same time be within reach of the Grid User‰s technical capabilities.

Since Grid User‰s installations are built to operate for a few decades, it is essential that the Connection codes are designed to anticipate the operational needs of the future system. Having this perspective in mind, the RfG NC and DCC NC set out requirements for the technical capabilities of generation and demand to ensure power system security and safety.

Differentiation by type of Generating Facilities

For a systematic and consistent addressing of the Generating Facilities in the requirements, and in order to reach consistency in the terminology used and appropriate cross referencing between the OS NC and the RfG NC, the OS NC has adopted the differentiation by type of Generating Facilities defined in the RfG NC in the following manner:

a)A Synchronous Power Generating Unit or Power Park Module is of Type A if its Connection Point is below 110 kV and its Maximum Capacity is 0.8 kW or more;

b) A Synchronous Power Generating Unit or Power Park Module is of Type B if its Connection Point is below 110 kV and its Maximum Capacity is at or above a threshold defined by each Relevant TSO This threshold shall not be above the threshold for Type B Power Generating Modules according to table 1;

c) A Synchronous Power Generating Unit or Power Park Module is of Type C if its Connection Point is below 110 kV and its Maximum Capacity is at or above a threshold defined by each Relevant TSO. This threshold shall not be above the threshold for Type C Power Generating Modules according to table 1;

d) A Synchronous Power Generating Unit or Power Park Module is of Type D if its Connection Point is at 110 kV or above; .a Synchronous Power Generating Module or Power Park Module is of Type D as well if its Connection Point is below 110 kV and its Maximum Capacity is at or above a threshold defined by each Relevant TSO. This threshold shall not be above the threshold for Type D Power Generating Modules according to table 1.

Synchronous Area	Maximum capacity threshold from which on a Power Generating Module is of Type B	Maximum capacity threshold from which on a Power Generating Module is of Type C	Maximum capacity threshold from which on a Power Generating Module is of Type D
Continental Europe	1 MW	50 MW	75 MW
Nordic	1.5 MW	10 MW	30 MW
Great Britain	1 MW	10 MW	30 MW
Ireland	0.1 MW	5 MW	10 MW
Baltic	0.5 MW	10 MW	15 MW

[Source: "Network Code on Requirements for Grid Connection Applicable for All Generating Facilities", ENTSO-E]

Table 1: Thresholds for Type B, C and D Power Generating Modules

3.7 WORKING WITH STAKEHOLDERS & INVOLVED PARTIES

The legally binding nature of network codes achieved through the Comitology process implies that they can have a fundamental bearing on stakeholders businesses. As such, the ENTSO-E recognised the importance of engaging with stakeholders at an early stage, involving all interested parties at the earliest possible phases in the development of the code, in an open and transparent manner.

ENTSO-Eôs stakeholder involvement comprises workshops with the DSO Technical Expert Group and public stakeholder workshops, as well as ad-hoc meetings and exchange of views with all interested parties as necessary.

Due to the many questions concerning the function of the Transmission System from an operational point of view that arose during the public consultation of the RfG NC, the first õunofficialö ENTSO-E stakeholder workshop on System Operation was held on 19th March 2012 in Brussels with an aim of explaining the key concepts in and around System Operation. A further aim of the workshop was to present information focusing on the operation of an interconnected Transmission System, and the physical basis for scoping and drafting the System Operation network codes. Stakeholders have also had the opportunity to raise questions, express feedback and expectations.

In line with suggestions by stakeholder organizations and following requests by the EC and ACER, ENTSO-E has scheduled four õofficialö workshops with the DSO Technical Expert Group and four õofficialö workshops with all stakeholders before, during and after the public consultation:

- The aim of the first OS NC Workshops (20th April 2012) was to present and discuss the scope of the draft OS NC, which reflected the work completed by TSO experts as of 5 April 2012. The workshop addressed the scope of the network code, provided an update on the present state and allowed for discussion and a Q&A session. Stakeholders in attendance included DSOs, industrial electricity consumers, generators, energy traders and turbine suppliers.

- The aim of the second OS NC Workshops (2nd July 2012) was to present updates made to the network code and to present the main content of the first version of this Supporting Document based on the stakeholder feedback received in the first OS NC workshop. The workshop was an opportunity for stakeholders, including DSOs, industrial electricity consumers, generators, energy traders and turbine suppliers, to provide feedback on the current status of the network code.

- The aim of the third OS NC Workshops planned during the public consultation will be to discuss in detail the remarks by the respondents in the consultation and to explain any outstanding issue or questions on System Operation or Operational Security, which might be raised by the respondents.

- The aim of the fourth OS NC Workshops planned for the 20th December 2012 will be to present the final version of the OS NC including the relevant amendments resulting from the public consultation.

4 Relationship between the OS NC & Framework Guidelines

The OS NC sets the pan-European basis for ensuring on a high level secure and coordinated System Operation, facing the three key challenges identified by the SO FG:

- To define harmonised Security Criteria.
- To clarify and harmonise TSOs roles, responsibilities and methods.
- To enable and ensure adequate data exchange.

The requirements described in the OS NC have been formulated in line with the SO FG and the new developments on System Operation, with the aim of maintaining the necessary level of Operational Security. The OS NC can therefore be defined as a benchmarking for the objectives and key challenges addressed in the Framework Guidelines: the Operational Security issues raised by the FWGL SO are addressed in eleven categories of requirements and these are further described in section 5 of this document.

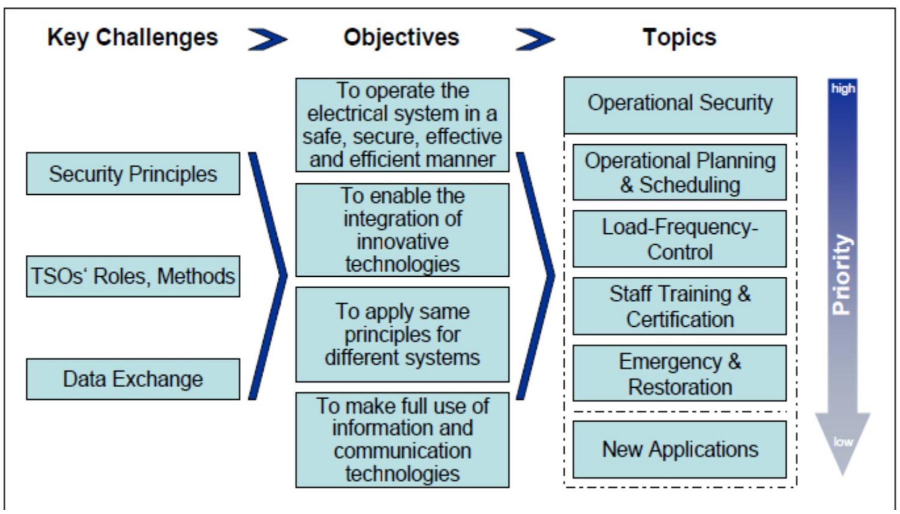

Figure 3. Structure and development flow of the Framework Guidelines on Electricity System Operation.

The OS NC reflects the common issues described by the OPS NC and the LFCR NC with the following reasoning:

- The bases of OPS including the principles, key tasks and activities conducted prior to the real-time operation are set out in the code, whereas the description of further details is part of the OPS NC.
- Whereas article 7 of the OS NC sets the general framework for the frequency control management, it is in the LFCR NC where concrete issues are described in greater detail.

As an instrument required for the maintenance and further improvement of normal operation and whose importance was emphasised in the ERGEG Guidelines of Good Practice for Operational Security [4], it has been considered appropriate to address the topic of Operational Training and

Certification in the OS NC with a general focus and with its own chapter(5). More details regarding Training will be developed within a separate NC on Operational Training and Certification.

Emergency and Restoration, as an issue focusing on defence plans and restoration of the system after a major disturbance or a blackout, but also analysing events afterwards, has been considered to be beyond the framework of a ñregularò System Operation. Thus it will be addressed separately in a later NC on Emergency & Restoration.

5 PROVISIONS OF THE OS NC

This chapter describes for each provision of the OS NC the objectives that the Network Code sets out to achieve by means of the defined standards and requirements:

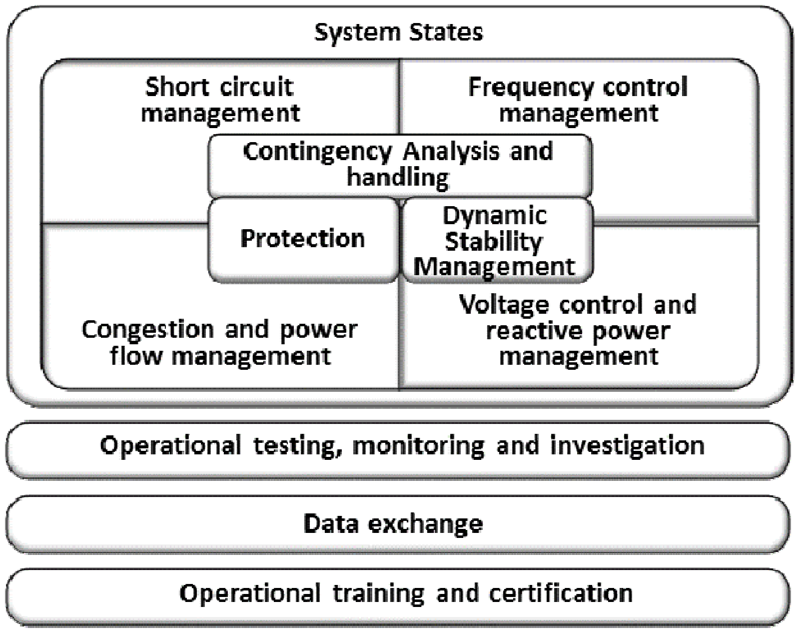

Figure 4: Structure and provisions of the Operational Security Network Code

5.1 SYSTEM STATES

A continuous monitoring of the System State, based on the real-time measured values of operational parameters with permanent online mutual information about the System State within affected TSOs and with a common set of definitions for the states across all TSOs, provides for effective State Estimation and for control actions in order to keep the system in a Normal State or return to it as soon and close as possible in case of disturbances.

The increased system coordination achieved by monitoring the System State contributes to a coherent and coordinated behaviour of the interconnected Transmission System, both in each Responsibility Area and between Responsibility Areas.

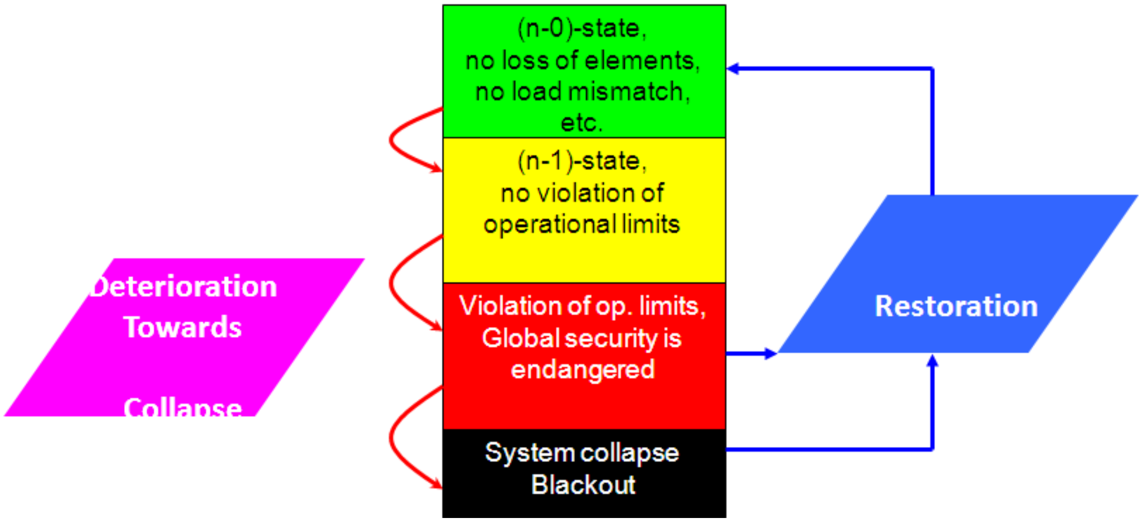

Figure 5: System States in the framework of the OS NC

5.2 Frequency Control Management

The scope of frequency control management is to maintain a continuous balance between generation and demand, ensuring frequency quality and stability within each Synchronous Area. For this purpose, TSOs shall procure adequate upward and downward active power reserve and shall define criteria, according to which the quality and stability of the frequency shall be assessed. What's more, in line with the NC on LFCR and the NC on Balancing, common criteria are set for the dimensioning and establishment of control reserves.

TSOs should be aware of parameters that can lead to frequency deviations and check them in order to take joint measures to limit the effects on their system balance. Increasing power exchanges between LFC areas, the intermittent nature of the RES generation and, the difficulties in forecasting load/generation variations due to normal operation evolution and/or disturbances, market driven imbalances – e.g. ramping at the hour shift- impose great challenges on the TSOs for balancing demand and generation. Furthermore, the robustness of the system in terms of stability is deteriorating, as the increasing volume of power stemming from RES does not contribute to the total inertia of the system. To the contrary, RES replaces synchronous generators and therefore alters the principles of the current power system operation.

5.3 Voltage Control and Reactive Power Management

Voltage conditions in a Transmission System are directly related to the reactive power situation at the system nodes. In order to compensate for an excessive consumption of reactive power, TSOs must make sure that the most efficient and effective producers feed / absorb sufficient reactive power onto the networks in addition to the reactive power from other devices installed in the networks or in Customer Facilities. TSOs must ensure a continuous and local reactive power balance to ensure a proper voltage level at the network.

In this context, the goal of voltage control and reactive power management is to ensure that:

- Voltage levels, reactive power flows and reactive power resources are monitored, controlled and maintained in real-time within the Operational Limits, in order to protect the equipment of the Transmission System and ensure its voltage stability.
- Adequate instantaneous reactive power reserve is available in spinning generators, reactors and capacitors in order to secure the technical functioning of the power system and to restore the Normal State after disturbances.

For this purpose, permanent online mutual observation and information exchange that takes place with neighbouring TSOs is established.

5.4 SHORT-CIRCUIT CURRENT MANAGEMENT

Short-circuit current management is required to prevent all types of Generating Facilities, network elements and related equipment from damage and to provide safety for persons, through the fast and selective disconnection of short-circuit faults.

The objective of short-circuit current management is therefore to keep the impact of short-circuit currents at a level that provides secure functioning of the Transmission System with system protection and its set-points. This implies:

- Enabling an accurate short-circuit current calculation by TSOs while following standardised principles and ensuring the required data provision from neighbouring TSOs, DSOs and Significant Grid Users.
- Monitoring the short-circuit currents and taking preventive and curative remedial actions if the Operational Security Limits are or tend to be violated.
- The required provision of information and communication to affected TSOs, DSOs and Significant grid users in order to be able to consider the effect of other Transmission and Distribution systems.

5.5 POWER FLOWS MANAGEMENT

Each Transmission System element has an operational power flow limit. These limits are defined with the aim of protecting the equipment and the people in the vicinity, also taking into account the technical constraints of the materials in order to avoid damage or premature ageing.

The scope of congestion and power flow management provisions is therefore to establish the operational means to maintain power flows below operational power flow limits on every part of the Transmission System. To be able to monitor and control operational parameters in the system it is necessary to have precise information about System States and an accurate State Estimation. For this, each TSO has to control operational parameters inside its own Responsibility Area and, with coordination, take into account the Observability Area of neighbouring systems; this implies structural and real time data information exchange between affected TSOs and between TSO and DSOs in its Responsibility Area. When necessary, individual or coordinated Remedial Actions shall be prepared and/or applied to avoid violation of Operational Security Limits.

5.6 CONTINGENCY ANALYSIS AND HANDLING

Article 11 of the OS NC covers the N-1 security principle, a long established deterministic standard which is common amongst TSOs. With the aim of maintaining the Operational Security of the

Transmission System, contingency analysis consists of simulating the tripping of network elements. This analysis is conducted based on the observability areas of the TSOs, respecting Operational Limits whilst preparing and carrying out pre-fault and / or post-fault remedial actions where required.

The key principles to be followed in relation to contingency analysis, which also outline the overall goals and objectives of contingency analysis in real-time and in operational planning phase are:

One goal

ñNo cascading with impact outside my borderò

Two obligations

1 - Obligation for each TSO to monitor the consequences of the events defined in its contingency list (= normal + exceptional contingencies) and warns its neighbours when its own system is at risk at any operational planning stage and in real time

2 - Mandatory coordination by bi-multilateral, even regional actions to better assess the consequences of any domestic TSOôs decision

Three behaviours

1 - ñBe aware of the risksò, even if not sufficiently covered by remedial action due to too high costs (potential emergency situations)

2 - ñBest effortsò to set-up remedial actions, that is not always possible or sufficiently efficient by one single TSO to cover exceptional contingencies

3 ï Be aware of impacts of domestic operational decisions (switching, redispatching, outage planning, capacity assessment) on neighbouring systems

Risk assessment: a concern

Each TSO is only responsible for the operation of its own network. But it is required to inform relevant neighbours in case it assumes some risks to come from outside or to come from inside to be propagated abroad.

Inter-TSO coordination

Bilateral, multi-lateral or regional coordination is requested to assess risks.

Thus, the objectives of contingency analysis and handling in the OS NC can be summarised:

- To ensure prevention and/or remedy in terms of control actions required to maintain Operational Security, for all credible contingencies affecting the Transmission System.
- To coordinate both analysis and control actions, wherever it is necessary, to ensure the best result ï Operational Security of own and the interconnected Transmission System.
- To rely on adequate data and information: real-time, forecast, Common Grid Model and sufficient exchange between TSOs and especially from DSOs and Grid Users.
- To elaborate pan-European standard provisions for Contingency Analysis in order to maintain Operational Security while maximizing system utilisation.

5.7 PROTECTION

Equipment protection is used to protect transmission assets from faults. System Protection Schemes are used to detect abnormal system conditions and take predetermined, corrective actions to preserve system integrity and provide acceptable system performance. System Protection Schemes are nowadays widely used by many TSOs in most Synchronous Areas.

System protection functions shall be analysed, with relevant network calculations, considering correct and incorrect functioning. If unacceptable consequences are forecast, functionality and redundancy of the scheme have to be accordingly adjusted to fulfil system security requirements. The functionality and operational status have to be monitored, communicated and coordinated between neighbouring TSO and other parties affected by the system protection.

5.8 DYNAMIC STABILITY MANAGEMENT

a) Objectives of the OS NC

The goal of the Dynamic Stability Assessment (DSA) is to ensure awareness of the TSO staff regarding the current and future planned operating state of the Transmission System with respect to stability, in the N situation and the potential (N-1) situation. In addition, DSA supports the decisions in relation to the most effective and efficient remedial actions to be initiated to prevent disturbances or correct their consequences if disturbances occur.

The extensive use of DSA allows different applications, not only in real-time operation, but also in operational planning phases. An emphasis must be put on training of staff operating and making use of DSA as well as to the continuous maintenance of models and simulation engines via on site tests and validations.

b) Added values of implementing the OS NC

The OS NC focuses on the different scopes that can be taken for the DSA depending on the characteristics of the correspondent Transmission System:

Presently DSA is only an issue for a few Transmission Systems where closer to real-time DSAs are required (e.g. Nordic countries due to a system characterised by longer transmission lines). However, the future evolution of DSA will focus on its connection with Special Protection Schemes and Wide Area Measurement Systems, in order to face operating conditions for which fast automatic remedial actions are necessary and cannot be achieved through the manual intervention by the control room operator. In this framework, Dynamic Security Analysis will indicate, in relation to automatic protection systems, the most suitable adaptive logics to be triggered in case of critical contingencies, calling for fast emergency corrective actions.

5.9 OPERATIONAL TRAINING AND CERTIFICATION

a) Objectives of the OS NC

In line with SO FG [1] and the Guidelines of Good Practice for Operational Security [4], operational training is required in order to guarantee that System Operators and other operational staff are skilled, well trained and certified to operate the power system in a secure way during all operational situations.

In this context, the OS NC sets up the goal of implementing a wide training and certification process, which will enable recognising and responding to abnormal operating conditions in appropriate timescales and, where appropriate, in a coordinated manner with other TSOs. Whatös more, the application of operational standards can be ensured by the development of programmes involving initial training, continuous staff development and regular certification re-assessment.

b) Added values of implementing the OS NC

The OS NC strengthens and formalises existing best practice amongst TSOs in training and certification thereby ensuring minimum standards are applied across all TSOs in ENTSO-E:

The OS NC sets up the obligation on TSOs to have in place continuous development programmes for their control room staff and to co-ordinate and co-operate on inter-TSO training for wide area transmission issues. Highly trained TSO staff are able to operate efficiently in the balancing of the Transmission System, whilst maximising the opportunity for cross-border transfers both of which deliver real economic benefits to customers, significantly in excess of the incremental costs of investing more in the training of TSO control room staff.

In addition, an on-going commitment to continuous development programme for control room staff will ensure TSOs can maximise the output from intermittent generation whilst maintaining security of the transmission system operation in an ever increasingly dynamic and changing future.

Furthermore, investing in TSO control room staff training will reduce the probability of widespread disturbances and disruption to supplies from unplanned events that if they occur can last for many hours or even days and for which the costs to the wider economic and social activity can be measured in billions of Euros.

The requirements set out on TSOs, DSO and Grid Users in this topic are building upon the existing best practice and identified needs.

6 NECESSARY DATA AND INFORMATION FOR SAFEGUARDING THE OPERATIONAL SYSTEM SECURITY

The present chapter achieves to justify the requirements set in the OS NC with regards to Data Exchange while evidencing the tasks of the TSO for safeguarding the system security and further describing why there is a need of establishing a coordinated information flow between TSOs, DSOs and System Users.

6.1 INTRODUCTION

As a consequence of the new developments on System Operation described in section 0, the increase of volume and dynamics of intra- and inter-regional power flows has significantly affected the security of System Operation. This tendency is set to further increase in the near and longer term future. What's more, the increased variable and dispersed generation on medium and low voltage levels replaces conventional generators in operation and this increases the TSOs challenges in managing the Transmission System in a safe and secure manner.

To underpin the security and stability of the electricity supply system, it is essential to assess the expected power flow in the transmission network as accurately as possible and to forecast the System State in order to avoid hazardous situations in real-time and to plan adequate measures. The required access by TSOs to data from DSOs and Grid Users has to be assured to facilitate this assessment by TSOs. Additionally, the OS NC covers the required access by DSOs to data from Grid Users directly connected to their Distribution Network in order to ensure security of supply.

For a high forecast accuracy, to ensure the security of the electricity supply system in the Responsibility Area at maximum capacity utilisation and as an issue that directly influences operational planning and System Operation, it is critical to be able to accurately forecast all parameters of the network model and the system balance. While the TSO carries out the topology forecast on its own, the power balance creation requires both its own grid information and that of Distribution Networks. The accuracy of variable generation forecasts can be significantly improved closer to real-time operation, which heightens the focus on the data and information to be provided by TSOs, DSOs and Grid Users.

Due to the full unbundling introduced by the 3rd Energy Package, there is no reason for the avoidance of data provision to a TSO due to confidentiality matters.

Thus, the focus is on fast feasible data provision by DSOs and Grid Users necessary for detecting, forecasting and thus for carrying out Security Analysis of a transmission system ahead of and in real-time, making possible increased coordination in System Operation between TSOs, DSOs and Grid Users.

The question of which partners have to provide which data for the Transmission System Operation in the respective Responsibility Area has not been clearly and consistently answered yet in the European context. The requirement of a binding answer seems evident taking into account the emerging system development of the European Electricity Supply[3] and the associated risks or disturbances that need to be handled by TSOs in order to ensure the conditions for maintaining Operational Security throughout the EU.

6.2 Tasks of the Transmission System Operators

The risks or disturbances that need to be handled by TSOs in order to maintain the security and reliability of the electricity supply system include at least the following aspects:

- Continued power supply of the customers connected to the transmission grid,
- Power flow control to avoid congestion,
- Frequency stability,
- Voltage stability,
- System stability and
- Grid restoration.

With regards to the exclusive responsibility of the TSO for system security and liability for its own actions, TSOs work on the principle that they must have full control over the tools used and a complete overview of the data quality in-house and externally-supplied information. Since mere trust in the accuracy of information without an appropriate level of assurance and control is not acceptable for reasons of liability, the OS NC establishes the right to TSOs to receive the required data with the aim of enabling the performance of accurate security analysis and, at the same time, establishes the obligation on Stakeholders and involved parties to provide the therefore required data with an adequate level of quality and precision.

With regards to the assumption of the system responsibility and herewith to the detection and prevention of short-term risks and disturbances, the Operational Planning and System Operation processes seem to be particularly crucial.

With regards to the task of maintaining the frequency stability, it is important to note that the responsibility of the TSOs includes their own Transmission Network, as well as the LFC Area as a whole, and thus the underlying network. This acquires special relevance in countries where a so-called cascading structure of Transmission and Distribution Network levels does exist, what e.g. is the case of Germany or Austria,

[3] See Section 3.5 for further details.

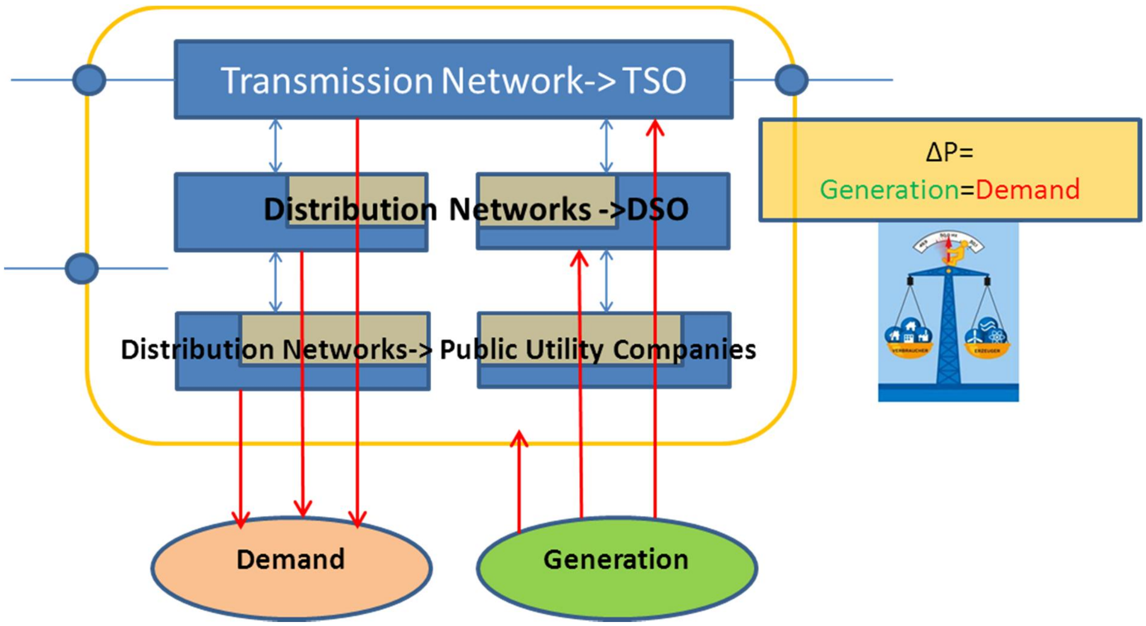

Figure 6: Schematic representation of a LFC area

This shows that the system responsibility linked to the task of maintaining the frequency control extends to the entire balancing area of the LFC Area at all grid levels, especially since effects leading to the disturbance of a power balance are generally not caused by the own grid operation but by the behaviour of the grid users.

Interventions by DSOs in the operation of customer installation plants represent an exception to the latter, e.g. regarding the avoidance of congestions in the Distribution Network. Especially these interventions are very complex in terms of their impacts on the Transmission System Operation and can influence with their effect on the system balance and load flow up to other LFC Areas.

Insofar it is essential that the TSO is informed in an appropriate manner about the current and planned grid user behaviour and the security interventions by DSOs in the whole LFC Area.

Since the TSOs work closely together on a horizontal level, each TSO has to ensure in its LFC Area that effects with negative consequences on system stability due to the close interconnection of European Transmission Systems do not lead to impacts on supra-regional or even European scale.

6.3 THE OS NC AS A PLACEHOLDER OF THE TOPIC DATA EXCHANGE FOR OPERATIONAL PURPOSE

The purpose of the Chapter Data Exchange is to define the data and information required by the TSO to perform its tasks described in the Network Code. The OS NC is the umbrella code of the SO NCs. Therefore, it has to consider all the possible data needed to guarantee the security in the System. This includes: real-time data, schedules, structural data and other possible data needed for analysis.

Part of this data may also coincide with data required in other network codes like the CACM NC. This is due to the fact that Operational Security is something inherent to the System. For example, the capacity calculation is a specific kind of security analysis focused on the border of Responsibility Areas.

6.4 THE TWO WAYS OF EXCHANGING DATA WITH THE TSO SET BY THE OS NC

In the OS NC, two possibilities are conceived for the TSO to receive data from Significant Grid Users, generators and demand facilities, connected to the Distribution Network. Both possibilities are already implemented processes within the European TSOs: Whereas one option is that SGU send the data directly to the TSO, the other option is that SGU send the data to the operator of the Distribution Network Operator who, at the same time, will forward them it send the data to the respective TSO.
The first option makes communication between TSO and SGU faster and more reliable as it is direct between both agents. The second one is simpler for SGU as sometime they would only need one communication link instead of two. This will only apply in those cases were the SGU do not need and do not have yet a communication link with the TSO.

As the two options conceived by the OS NC are already in use and properly working, allowing both of them is the simplest and most economic option. Reducing the possibilities will oblige agents in some places to modify their installations. That will mean new costs.

7 COMPLIANCE, TESTING AND INVESTIGATION IN THE FRAMEWORK OF THE OS NC

7.1 COMMON TESTING AND INCIDENT ANALYSIS RESPONSIBILITIES

7.1.1 The goal of Operational Testing and Monitoring

Operational testing and monitoring is aimed to ensure correct functioning of elements of the Transmission and Distribution System and Grid User's equipment; to ensure Generating and Demand Units continue to meet connection requirements and their declared capability and supply of ancillary services; to maintain and develop operational procedures; to train staff and to acquire information in respect of power system or equipment behaviour under abnormal system conditions.

Planning for and coordination of operational tests is necessary to minimise disruption to the stability, operation and economic efficiency of the interconnected system. For the efficient planning, coordination and implementation of tests, the TSOs require the cooperation of Grid Users in the provision of the necessary data. As the power system is subject to various disturbances that could lead to a widespread incident, the TSOs will have to undertake investigations to determine the main causes and learning points of disturbances in order to avoid, if possible, their recurrence.

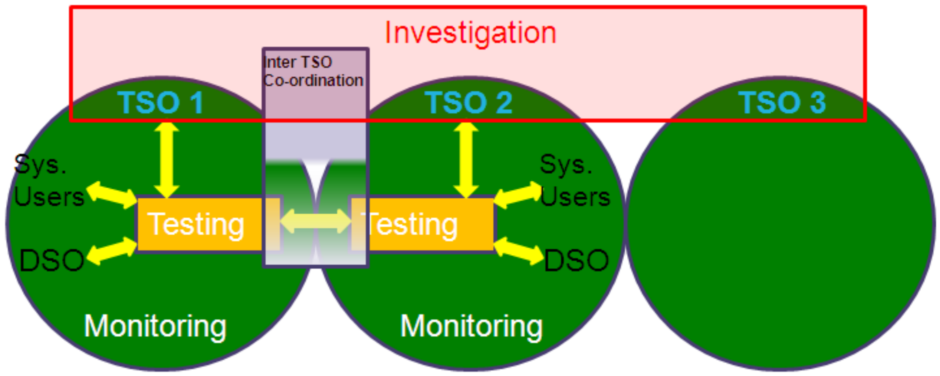

Figure 7: Coordination of tests between TSOs, DSOs and System Users

7.1.2 Common Testing and Incident Analysis Responsibilities in the framework of the OS NC

The chapter "Compliance, Testing and Investigation" of the OS NC is not replacing either redundant to the RfG NC. It should be noticed that the tests required in the RfG NC have the special purpose of certifying and are much more exhaustive due to their nature.
From the operational point of view, the tests required in the OS NC should be seen as complementary to the RfG NC: the OS NC deals with disturbances, faults and any other issue that can happen during the lifetime of the facility. The only one exception when the tests are repeated is in case of significant changes where it arises as necessary to repeat the compliance of those technical requirements set by the RfG NC.

7.2 THE INCIDENTS CLASSIFICATION SCALE

The Incidents Classification Scale developed by ENTSO-E [8] will provide the procedures for incident classification, analysis and reporting with the aim of monitoring system security levels and identification of improvements to reduce the risk of reoccurrence. The incidents classification scale rankes disturbances into four levels of severity, ranging from;

- Local events the consequences of which are limited to one TSO (Level 0);
- Noteworthy disturbances covering national events the consequences of which are manageable by one TSO (Level 1);
- Extensive and major incidents covering regional events (Level 2);
- Widespread incident and major incident for one TSO such as massive loss of load for one TSO, isolated system or regional black out (Level 3).

To identify the incident level, the following five general system reliability criteria have been defined:

- Transmission network equipment events (tripping of transmission grid equipment);
- Generation events (tripping of generators);
- Load events;
- Degradation in system operating conditions leading to non-fulfillment of the security criteria or violation of standards;

- System disturbance leading to a reliability degradation.

Different thresholds have been defined to take into account differences in the synchronous areas. Specific thresholds are defined for:

- The definition of loss of generation;
- The definition of loss of load;
- Frequency deviation; and
- Percentage of peak load affected by black out.

For example, for a Level 2 incident any of the following criteria apply:

- Transmission network equipment events: tripping with consequences at regional level (exchange capability and social consequences);
- Generation events: loss of generation in a time period of 30 minutes leading to a degradation of system adequacy, for Continental Europe >3000 MWs;
- Load events: all regions except isolated systems, disconnection of load on one TSO area of 10 to 50% of the load at the time of the incident;
- Degradation in system operating conditions: Emergency State transmitted by the ENTSOE wide awareness system;
- System disturbance leading to a reliability degradation:
    - Sustained frequency deviation below the last step of automatic load shedding, for Continental Europe 800 mHz ï 2 Hz;
    - Separation of a significant part of the grid (at least one TSO);
    - Regional (synchronous area) collapse.

The level of detail of the investigation/analysis will vary depending on their impact on the integrity of the interconnected system:

- For local or national incidents which have limited consequences with a low effect on reliability there will be no obligation to carry out specific analysis. These events will be reported to allow statistical analysis and TSOõs to report events for internal purposes.

- For national incidents which have noticeable consequences (high security and/or market influence or cause violation of standards for at least two TSOs) and are manageable by one TSO, analysis will be carried out if decided by a TSO, coordinated system operation or any type of working group dedicated to operational issues, ENTSOE Regional Group or the ENTSOE System Operations Committee. The relevant information will be shared among TSOs using the reporting tool and the analysis will be prepared by the impacted TSO covering the facts, actions, anomalies and learning points.

- For an extensive incident at a regional level (violation of standards, degradation of system adequacy, or important social consequences) not manageable by one TSO and wide area events such as massive loss of load (50% / 70%) on one TSO or regional blackout a detailed report will be prepared by an ENTSOE Regional Group team. An expert panel is appointed to perform the analysis based on a TSOõs (or a working group dedicated to operational issues) proposal, and approved by the ENTSOE Regional Group. The analysis will be performed in two steps. After collecting the data the expert panel will produce a factual (or preliminary) report. The aim of this report is to provide a clear understanding of the main causes, a clear description of the disturbance (situation before and after), preliminary evaluation of actions taken and functioning of equipment. The analysis (or final) report will include conclusions and recommendations (an action plan and lessons learned).

In addition to the data received via the SCADA system, the following information may be needed to fully investigate a major system incident:

- State of Network pre-fault/disturbance including details on any large angular differences open due to a line being out of service;
- Fault records from Disturbance Recorders and Relays;
- Relay Annunciation records;
- Event recordings from Transmission Stations/Significant Grid Users;
- Weather including any lightning activity (lightning locator);
- Information on action of Under Voltage Load Shedding/Under Frequency Load Shedding schemes and System Protection Schemes;
- Information from generators as to cause of generator tripping (e.g. flame out on a GT);
- Information from equipment manufacturer on cause of fault (e.g. bushing failure results/CT moisture ingress results etc.);
- Interviews with Network Operators & Control Room Operators;
- Customer load lost from DSO.

8 FUNDAMENTAL CONCEPTS & PROCESSES OF THE OS NC

This section presents the fundamental concepts used in the framework of the OS NC while trying to clarify at the same time resulting comments of stakeholders during the OS Network Code Development Process.

8.1 COMMON GRID MODEL (CGM)

7.1.1 What is the CGM?

The CGM is an ENTSO-E wide data set used to prepare a model which can be used to analyse different scenarios. These scenarios are valid to enable security analysis and capacity calculation to be performed. To perform the analysis, the whole Common Grid Model or the necessary part of it is used. The scenarios are prepared for different time frames: Year ahead, Week ahead, Day ahead and Intraday. All of them are used for Contingency analysis; and the Day ahead and Intraday ones are also used for Capacity Calculation.

7.1.2 What does the CGM comprise and how is it formed?

The CGM comprises at least the transmission system of 220 kV and higher voltage network, an equivalent model of the lower voltage grid with influence and the sum of generation and withdrawals in the nodes of the transmission network. It is formed by merging the individual data sets provided by every TSO as stated in the article 17(3) of the OS NC. The individual data provided by each TSO comes from its own observability models. The Individual data sets, so-called individual grid models, are part of the Common Grid Model, as reflected in the figure below:

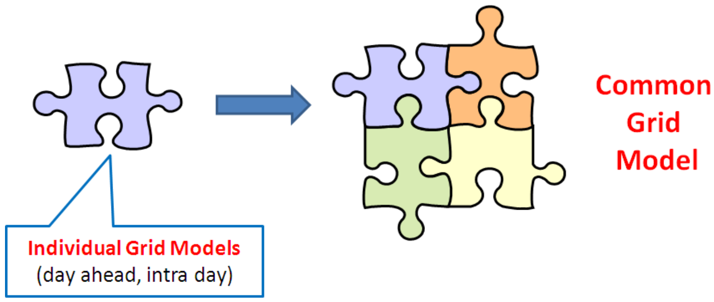

Figure 8: Individual Grid Models versus Common Grid Model

Whereas the OPS NC describes the procedure to prepare the CGM scenarios in each time frame for contingency analyses, it is in the CACM NC where the requirements for building the CGM scenarios for capacity calculation purposes are set.

7.1.3 Overview of the building of the CGM

The next figure gives an overview of the building of the CGM and whether the respective actions are performed on TSO level or coordinated on a regional level:

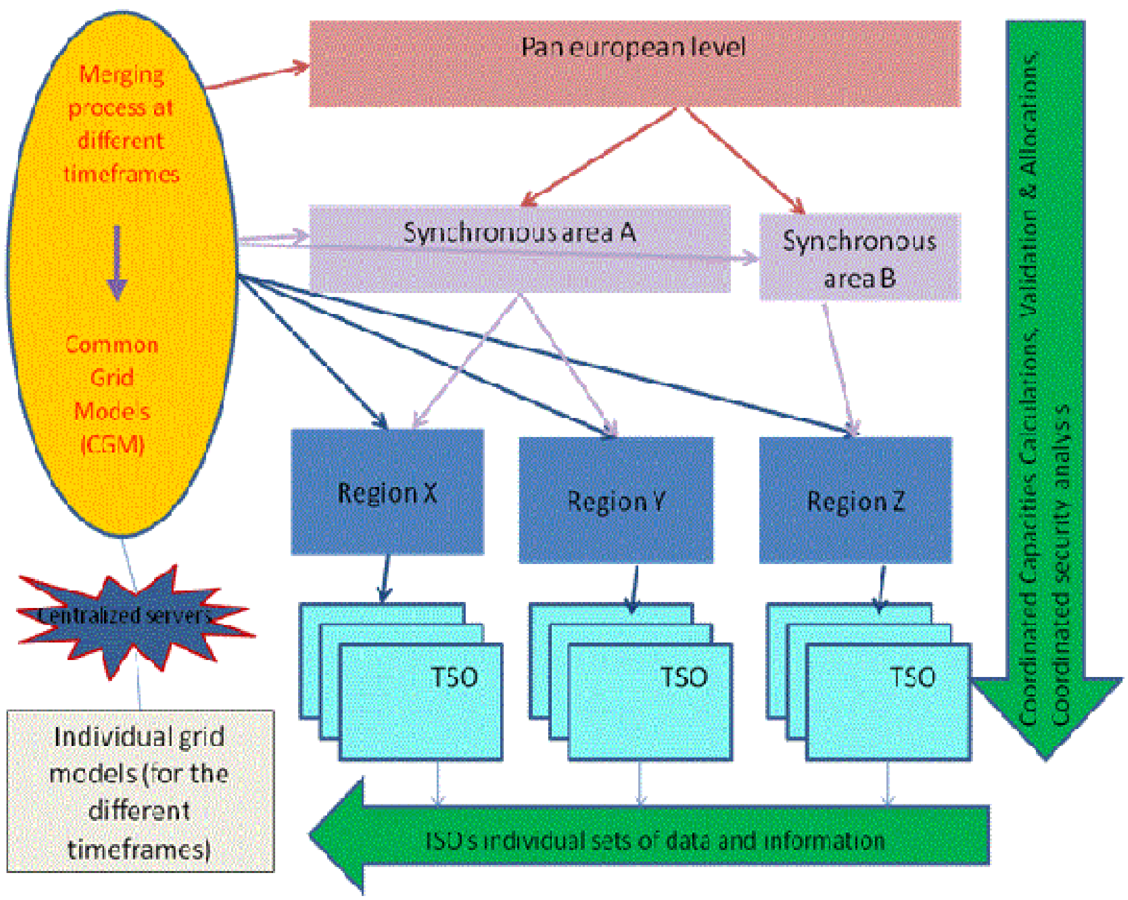

Figure 9: Overview of CGM building process: data and info exchange

The OS NC focuses on the Common Grid Model scenarios relevant for the purpose of security analysis; each TSO uses the data from its observability area to build, within each relevant time frame, the individual data set for the Common Grid Model. This process is carried out considering certain conditions and covering zones to allow coordinated security analysis such as congestion and power flow management. It has to include relevant characteristics of the connected generation, consumption and distribution and transmission equipment and take into account planned outages.

The data from its observability area within the relevant timeframe permits the TSO to monitor its system and to perform the contingency analysis in order to assess the system state for contingencies and to set up the required remedial actions.

8.2 SIGNIFICANT GRID USER (SGU)

According to the SO FG, Significant Grid User is defined as ñpre-existing grid users and new grid users which are deemed significant on the basis of their impact on the cross border system performances via influence on the LFC Areaôs security of supply including provision of ancillary servicesö. This has been the approach followed by the OS NC, defining the significance by considering the impact of a grid user on the cross border system performance, regardless of the connection point voltage.

Within the scope of this Network Code, the following shall be considered Significant Grid Users

a) New Power Generating Modules type A, B , C and D according to [NC RfG];

b) Existing Power Generating Modules whose Connection Point or Maximum Capacity is at or above the Thresholds defined in Article 6(3) of [NC RfG]. For the purpose of this Network Code, Existing Power Generating Modules shall be also classified as type A, B, C and D following the same criteria defined in Article 6(3) of [NC RfG] for New Power Generating Modules;

c) Existing and New Demand Facilities with the Connection Point to the transmission system;

d) Existing and New Demand Facilities providing Demand Side Response whose Maximum Capacity is equal or above 1 MW.

While respecting the provisions of Article 3(3), each TSO may define different thresholds of significance for Grid Users depending on the characteristics of the electric power system.

7.2.1 SGU: a unique concept of the Operational Codes

Significant Grid User means significant for operational matters such as the provision to the TSO or DSO of structural data, forecast output or consumption data, provision of real time data and other obligations such as requirement to follow a TSOs instruction to protect system security.

The term SGU is unique to the Operational Codes and differs from the term Significant Generating Unit used in the RfG NC, which primarily sets out the design and build capability requirements for different thresholds of generation size. It should be noted that the thresholds for SGU may:

- Not be the same thresholds as those used in the RfG NC: there will probably be different thresholds set for SGU-demand facilities and for SGU-generation facilities;
- Vary between TSOs or regionally and
- Need to be changed over time, in cooperation with the NRA as set out in article 3(3)).

A TSO will therefore seek to establish the highest possible thresholds for SGU to limit the impact and burden on its users that is consistent and justified by the need to maintain system security and their impact on cross border exchanges.

For example, a certain TSO may have a number of its DSO with only a few embedded generating units of size 3-10 MW and no significant congestion issues on the transmission network and so deem its thresholds for SGU for generation do not need to be down to a level of 3MW, whereas another TSO may have several DSO with many hundreds of generating units in these size ranges and without accurate structural, forecast and real time data from these units may not be able to adequately ensure system security.

This example evidences that the obligations on SGU from the OS NC may need to be set geographically to ensure the costs of meeting these obligations across the whole of the EU are minimised whilst the benefits to all users are maximised. In addition, over time the TSO with only a few embedded generating units may experience a rapid growth in the build of generating units in its DSOs networks in the range 3-10MW and so may need to seek to reduce its threshold levels to ensure they begin to provide the TSO with the information it now needs.

8.3 LFC AREA, RESPONSIBILITY AREA, OBSERVABILITY AREA,

7.3.1 Explanation of the different concepts

Load Frequency Control Area (LFC Area)

From a functional point of view, the term LFC Area is related to load frequency control, aiming to balance the LFC area in terms of frequency, including loads and generation. Therefore, a LFC Area fulfils the following functions:

- Being responsible for primary frequency control within its territory;
- Being able to maintain power interchange at the scheduled value;
- Cooperating to restore frequency to its set value following a perturbation;
- Being responsible for accounting inadvertent energy deviations within its territory;

Therefore, in the framework of the LFC NC, Load Frequency Control Area appears defined as follows:

“A part of the Synchronous Area physically demarcated by points of measurement of Tie-Lines to other LFC Areas fulfilling the Area Process Obligations of a Control Area;”

Responsibility Area

Being defined as follows in the OS NC:

“A coherent part of the interconnected system operated by a single TSO with physical loads and generation units connected within the area”,

The term Responsibility Area covers a little greater part of the system than the term LFC Area: the TSO is responsible for maintaining the N-1 principle of its own grid and all the interconnectors to adjacent TSOs. The equipment comprising this network is called Responsibility Area.

Introducing the concept of Observability Area

Due to the increase of interconnections between TSOs, security assessment has become more and more interdependent. As a consequence the TSO has to take into account the influence of the surrounding grid on its Responsibility Area by analysing the external transmission network which has influence on its Responsibility Area. This introduces the concept of Observability Area, which includes the Responsibility area, and is defined as follows by the OS NC:

"Observability Area means the area of the relevant parts of the Transmission Systems, relevant DSOs and neighbouring TSOs, on which TSO shall implement a real-time monitoring and modelling to ensure reliability of the respective Responsibility Area."

The following figure reflects in a schematic way the concepts of Responsibility Area and Observability Area with the purpose of clarifying what is exactly meant under each term and how are those terms linked:

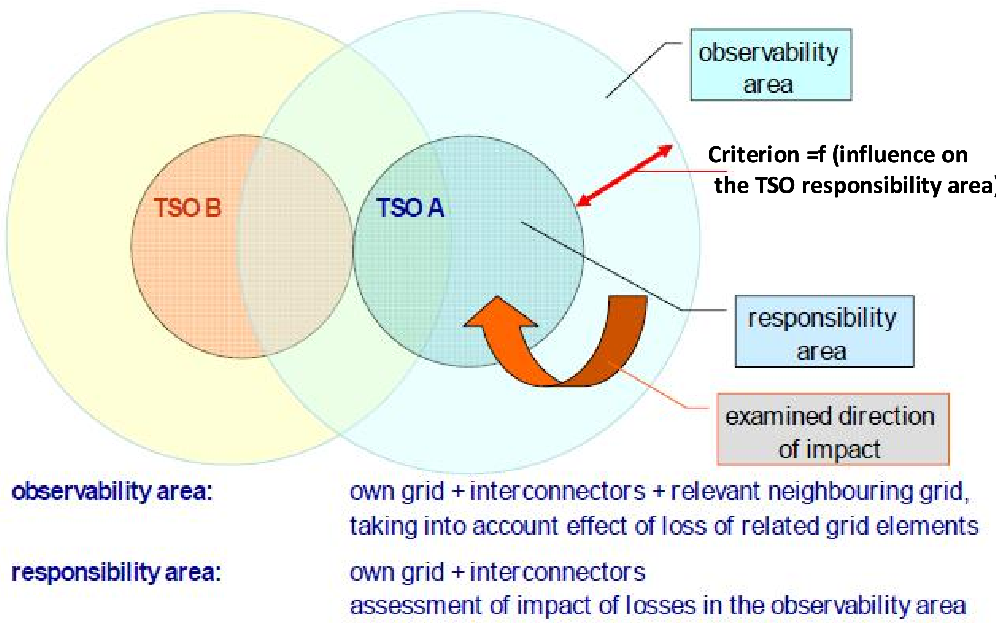

Figure 10: Definitions on Observability Area and Responsibility Area of a TSO

8.4 N-1 PRINCIPLE

8.4.1 (N-1)-assessment: classification of contingencies as a function of probability of occurrence

The classification of the contingencies in ordinary, exceptional and out-of-range for the purposes of the (N-1)-assessment is based upon the probability of occurrence of each contingency. Thus, contingencies with a high probability of occurrence are characterised as ordinary, the ones with a low probability are characterised as exceptional and those with an

extremely low probability are characterised as out-of-range. For example, the single loss of a line has a high probability of occurrence and therefore belongs to the ordinary contingencies. On the other hand, the simultaneous loss of multiple elements is considered to be of lower probability and is therefore normally either in the exceptional or in the out-of-range category. Factors such as the severity of the incident and the resulting duration of the unavailability of the element due to the contingency are not taken into account in the formation of the contingency list.
One such example is the tripping and damage of one or more generators due to the occurrence of a resonant frequency in the synchronous interconnected system. Such an incident is highly severe, as it damages the turbine-generator system und results in a prolonged period of unavailability of the generators due to demanding repair works. However, such a contingency is considered as highly improbable, as each generator is equipped with automatic protection systems, which disconnect the generator from the system much before the deteriorating frequency reaches the resonant frequency.

8.5 SYSTEM STATES

8.5.1 Common Awareness System

The origin of the European Awareness System: UCTE incident report 09/11/2006

- **Conclusions**:

  ñDuring the first minutes of disturbances, dispatchers should focus their actions on the restoration of normal conditions. On the other hand, the information about localisation of the source of the disturbance and overall system conditions is necessary for other TSOs in order to act accordingly and efficiently. On November 4, this was true more than ever - the information about the split of the system into three areas was available to some operators with significant delay. This issue might be solved via a dedicated central server collecting the real-time data and making them available to all UCTE TSOs. In this way, each TSO will obtain within a few minutes essential information about disturbances, beyond their own control area.ò

- **Recommendation #4**: ñInformation platform allowing TSOs to observe in real-time the actual state of the whole UCTE system in order to quickly react during large disturbancesò.

What is an Awareness System?

An Awareness System is a tool whose objectives are:

- *In case of a stressed situation*: to provide automatic or manual information shared to enable the TSOs to apprehend globally an endangered situation,

- *In case of disturbance*: to provide information to the TSOs to help them to identify its origin and its borders.

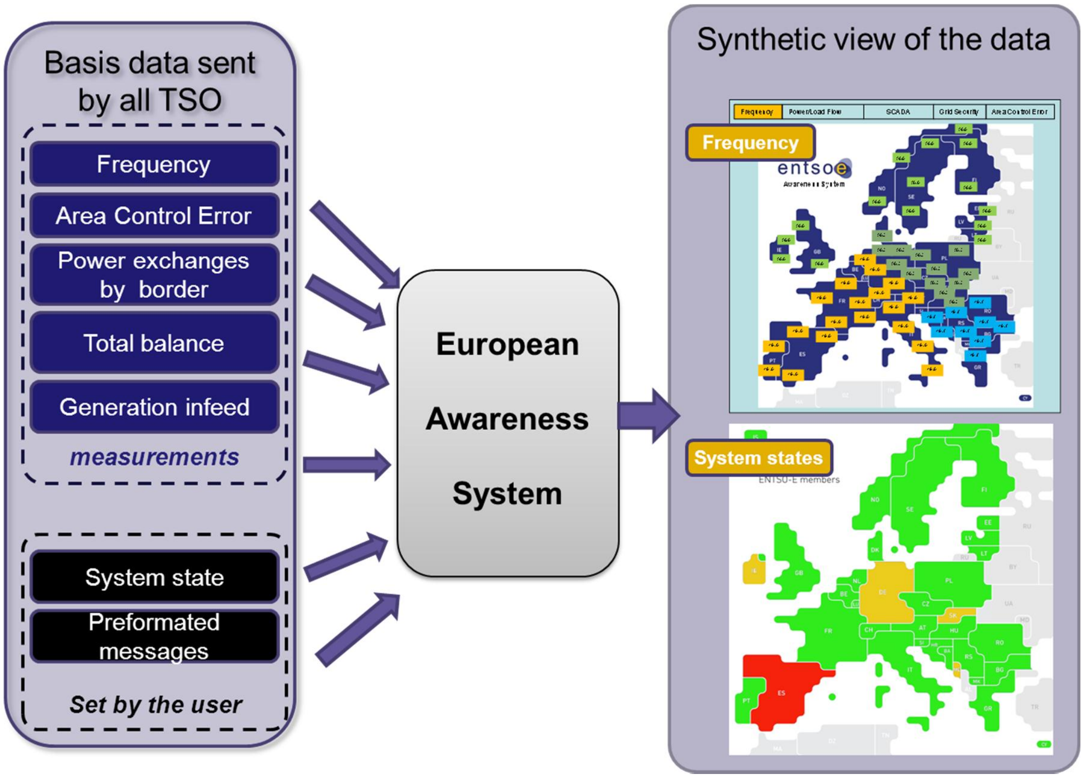

Figure 11: European Awareness System (EAS)

Data available in the European Awareness System (EAS)

In the following, the parameters available in the EAS are presented. For each of those parameters, the indications aimed to achieve by the EAS are briefly summarised.

- *Frequencies:*
    - Indication for actual overall active power balances in different synchronous areas / regions;
    - Indication for synchronism in the transmission grid regions;
    - Indication of possible existence of different asynchronous grid sections in one region (e.g. by identification of different frequencies in case of network split in the transmission system).

- *Area Control Error*

    - indication of sudden or persisting power imbalances during normal operation and after incidents;
    - indication, if (and for how long) certain values have not changed their sign, are in a certain range, exceed a certain limit, have a certain mean value for the last 15 minutes or fulfill other numerical conditions

- *Scheduled and measured power exchanges:*

- indication of sudden or persisting power imbalances during normal operation and after incidents;
- indication, if (and for how long) certain values have not changed their sign, are in a certain range, exceed a certain limit, have a certain mean value for the last 15 minutes or fulfill other numerical conditions.

- *Generation infeed*

    - Provide a common geographical ENTSO-E-wide real-time overview of the actual generation infeed in the ENTSO-E area.

Manual indications from the operator

System states

- Detailed definition of each System State to be set in the usage procedure is defined in Article 6 of the OS NC.

9 ADDED VALUES OF THE OS NC

While deciding on the objectives and major topics to be included in the OS NC, a constant screening process with the objectives defined by the SO FG has been carried out. The analytic approach taken for drafting the OS NC resulted in the current code structure. Reaching this point and by recognising that the added values of the code are inherently linked to its Provisions of the OS NC, the following benefits are to be expected by implementing the operational principles defined in the OS NC:

Added value	Related article of the OS NC
Apply the same operational security principles for System operation among European TSOs.	- The whole code
Improve the interconnected system safety and security.	- Articles 6 to 13
Optimise the detection of constraints in the Transmission System by enforcing coordination between TSOs and between TSOs, DSOs and Significant Grid Users.	- Articles 6, 11 - Chapter 3: Data Exchange
Reduce the risk of system-wide disturbances and the number of critical incidents, avoiding major incidents and limiting their consequences if they occur.	- Articles 6 to 13
Enhance uniform treatment of Significant System Users across Europe.	- Articles 6, 8, 11, 13 - Chapter 3: Data Exchange
Enable the integration of RES, maximising the output from intermittent generation whilst maintaining security of the Transmission System operation in an increasingly dynamic and changing future.	- Article 11 - Chapter 3: Data Exchange
Increase the potential for greater volumes of cross border exchanges, whilst ensuring existing levels of reliability are not reduced alongside ever increasing levels of RES intermittent	- Article 11 - Chapter 3: Data Exchange

output.	
Prepare the network for integrating distributed generation.	- Article 11 - Chapter 3: Data Exchange
Make efficient and effective use of smart grid applications.	- Chapter 3: Data Exchange
Provide the adequate conditions for exploiting the demand-side potential and integrating advanced power electronic systems.	- Article 32 - Chapter 3: Data Exchange
Improve conditions for data collection, handling and exchange.	- Article 5 - Chapter 3: Data Exchange
Provide a framework for the compatibility of tools.	- Chapter 3: Data Exchange, but mainly in OPS NC
Enhance the coordination of the tests between involved parties in order to ensure the correct functioning of all elements connected to the Transmission System.	- Article 32
Provide a common framework for the training of operators.	- Article 29

Whereas the benefits mentioned above cover the improvement of system security and therefore the ultimate goal of preventing blackouts, concrete numbers depend strongly on the underlying disturbance scenario and the region. Moreover, the probability of such events must be taken into account.

It is evident from this fact that a quantitative analysis of the added values of implementing the requirements of the OS NC would require an assessment, of the implementation and additional operation costs, to be conducted in cooperation by the TSOs, DSOs and Significant Grid Users.

10 SUMMARY OF CHANGES TO THE DRAFT NETWORK CODE

10.1 INTRODUCTION

This section of the document provides a summary of the comments received as a result of publication, via workshops and in discussion with stakeholders and regulatory authorities. It is intended to provide interested parties with an explanation of the most significant changes which have been made to the code.

10.2 SUMMARY OF COMMENTS

In total we received just over 1200 individual comments as part of the public consultation. Those comments were varied and, as shown in the diagram below, covered most parts of the network code. However, comments were mainly focussed on definitions, consistency with RfG, system states and data exchange in particular.

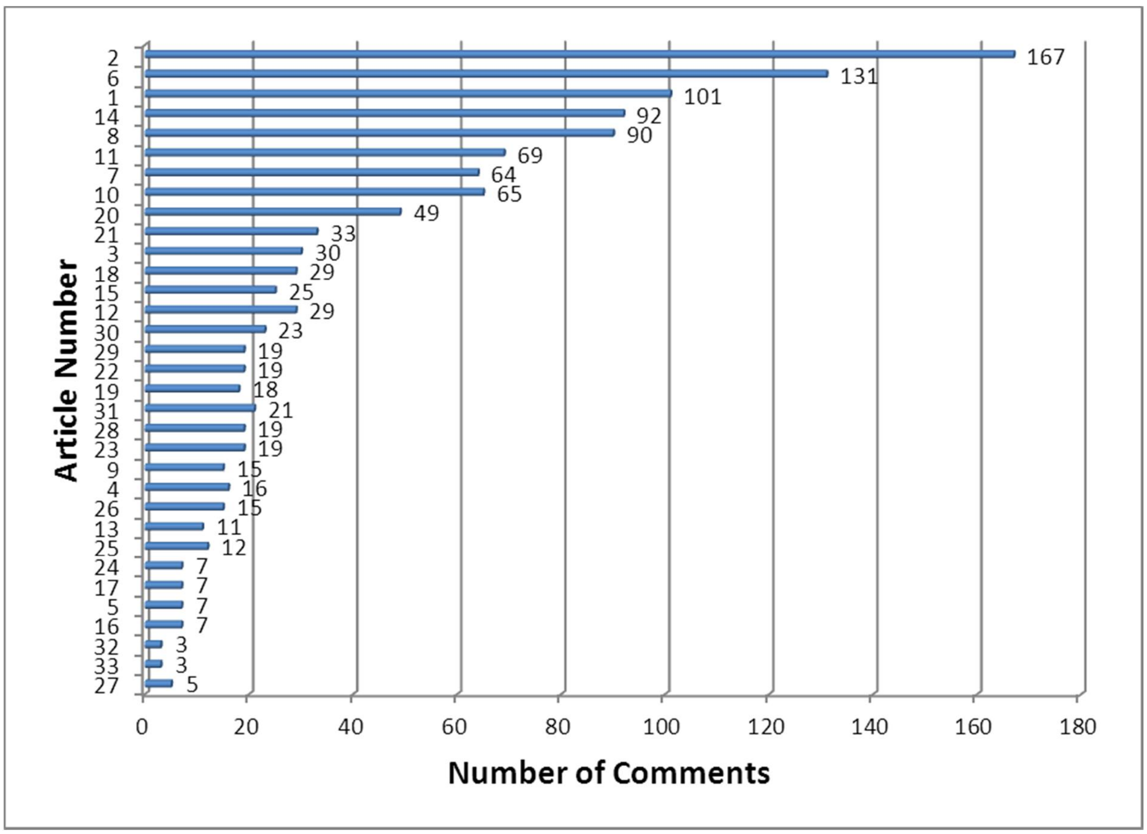

Figure 12: Analysis of articles by number of comments received

As the summaries demonstrate, each comment was considered and assessed and decisions were taken about whether there was a need to update the network code. Themes which occurred frequently in responses were:

Å There needs to be more transparency and consultation;

Å Asking for more NRAs involvement;

Å Asking for cost recovery issues for all stakeholders;

Å Provision should take into account human and nuclear safety;

Å More clarification on information exchange;

Å Remedial actions and involvement of DSOs;

Å Consistency with RfG and DC concerning disconnection of grid users at specified frequencies and voltages, and with other system operation NCs;

Å There is a new definition of significant grid users than in RfG and DCC and requirements to existing power plants;

Å On technical issues related to system security, e.g. ramping, reactive power, noncompliance with N-1, clearance time, connection point, minimal inertia, etc;

Å TSOs decision process to be clarified;

Å Cost benefit analysis for significant changes;

This list is by no means exhaustive and does not reflect the views of all respondentsó However, they are points where we were particularly encouraged to focus during the stakeholder workshops which were held during the public consultation.

10.3 STRUCTURAL CHANGES IN LIGHT OF COMMENTS

As we mentioned above, many of the comments we received focused on the need to increase clarity within the network code. We carefully considered these changes and made the following structural changes in the updated version:

Moving the Article 14 to the Chapter 6 Compliance as a new Article 32 Common testing and incident analysis responsibilities and proposed new articles on cost recovery, involvement of NRA in incident analysis and publication added, for Analysis of Quality of the grid connection point - clarification made, TSO and DSO to provide to information for Significant Grid User investigation, and some articles removed which are covered by the RfG and the DCC.

10.4 ENHANCING CONSISTENCY

We have sought to respond to comments about inconsistencies in the network code and have made considerable efforts to ensure it reads like a single document. Particular focus has been given to the following:

- Using of frequency and voltage limits defined in RfG NC and DCC NC in system operation and consistent with load frequency control in LFCR NC.

- Involvement of NRAs is coherent through all system operation codes. Several parties pointed out that these powers are set out in law (Directive 2009/72/EC, Articles 36 and 37). Given this concern we have updated the Article 3 in the first section of the network code. This refers to the powers of regulators from Directive 2009/72/EC and from the third energy package. It also presents a consistent set of timings and makes it clear where regulatory authorities have a role.

- Significant grid users are consistent with the significant users defined by RfG and DCC and including thresholds for existing users.

- Description of common grid model is consistent with requirements of CACM and OPS NCs.

- Concerning Transparency, a number of comments are asking us to make the TSOs decision process more open and clear. All information required by the new EU transparency guidelines will be published.

- Definitions are reviewed. Consistency across network codes being developed over a period of years is a considerable challenge. Nevertheless, we recognize the importance of consistency and have taken steps to improve definitions, to align them with those used in other draft network codes (or already existing legislation), and to take steps to ensure the definitions in OS NC can be used in future network codes.

10.5 Most Significant Content Related Changes to the Network Code

The points presented in section 10.4 have, in our view, improved the clarity of the network code, though have not introduced substantial changes relative to the draft which was consulted on. However, comments received via the consultation and through workshops and meetings led us to make a fairly large number of content related changes to the network code. Key changes are summarized below:

Regulatory Aspects – provision harmonized among system operation codes

Frequency Control Management and Voltage Control and Reactive Power Management – adding frequency and voltage operational limits

Data Exchange – Reviewed all articles to optimize the data exchange, avoiding duplication of data provision and to be consistent with the other NCs.

10.6 Conclusion

In our view, the changes discussed in this section have improved the overall consistency and readability of the network code and, as well as addressing a significant number of stakeholder concerns, have improved the overall quality of the network code and extent to which it complies with the framework guideline. Weꞌd like to thank the parties that responded to the consultation for their helpful views.

11 Next Steps

In this section we briefly summarise the main steps of the Network Code Development Process with a special focus on those which will occur between the submission of the OS NC to ACER and its application.

11.1 SUBMISSION TO ACER

Regulation (EC) No 714/2009, and in particular its Article 6, defines a clear Network Code Development Process.

The process begins with the set up by the Commission of an annual list of priorities amongst the 12 areas where Article 8(2) of Regulation (EC) No 714/2009 foresees the need for a NC. The annual priority list must be adopted after consultation with the relevant stakeholders.

Once a priority list is established, the Commission shall request ACER to develop and submit to it a non-binding framework guideline. The Framework Guidelines are intended to set clear and objective principles with which the Network Code should be in line.

The development by of a Framework Guideline is followed by a request from the Commission for ENTSO-E to develop a Network Code within a twelve month period. The Network Code to be developed by ENTSO-E within that period shall be subject to an extensive consultation, taking place at an early stage in an open and transparent manner.

At the end of these 12 months ENTSO-E delivers a Network Code and set of explanatory documents to ACER for its assessment.

11.2 THE ACER OPINION

ACER has three months to assess the draft prepared by ENTSO-E and deliver a reasoned opinion. In doing so, ACER may decide to seek the views of the relevant stakeholders.

ACER can decide to recommend to the Commission that it adopts the Network Code if it is satisfied that it meets the requirements of the Framework Guidelines or can provide a negative opinion; effectively meaning the code is returned to ENTSO-E.

11.3 THE COMITOLOGY PROCEDURE

The Network Code prepared by ENTSO-E shall only become binding if, after being recommended to the Commission by ACER, it is adopted via the Comitology procedure.

The Comitology process will be led by the Commission who will present the draft text to representatives of Member States organized in so-called “committee”. The Comitology procedure used for the network codes (called regulatory procedure with scrutiny) grants the European Parliament and the Council important powers of control and oversight over the measure adopted by the committee.

For that reason, it is unclear how much time the process can take in practice. Our working assumption is that it will take about 12 months from the issuing of the ACER opinion (if positive) to the conclusion of the Comitology process.

11.4 ENTSO-E STEPS DURING THIS PERIOD

Meeting the requirements of the OS Network Code is a significant challenge for ENTSO-E. During the period in which the Network Code is being considered by ACER and the Commission, we will continue work to prepare for the delivery of the requirements of the Network Code. Some of these requirements are particularly challenging and we feel that beginning work in the near term is necessary to delivering them on time.

11.5 ENTRY INTO FORCE

The OS NC will enter into force 20 days after its publication. All provisions of this Network Code shall apply as from the day of expiration of a two years period following its publication.

Because of uncertainties about the ACER opinion, the timings of the Comitology process, the time needed to deliver parts of the Network Code (the timings are ñno later thanò) and the time needed to approve parts of the Network Code (which could include a referral to ACER), it is not possible to say exactly when each requirement of the OS NC will exactly apply. A close working relationship between ENTSO-E, ACER, NRAs and the Commission is, in our view, necessary for ensuring the implementation of the OS NC as soon as possible.

12 REFERENCES

[1] ñFramework Guidelines on System Operationò (FG SO), ACER December 2011.

[2] ñInitial Impact Assessmentò, ACER June 2011.

[3] ñNecessary data and information for safeguarding the operational system security by the German Transmission System Operators according to Section 12(4) of the EnWGò, August 2011.

[4] ñGuidelines of Good Practice for Operational Securityò, ERGEG November 2008

[6] ENTSO-E, Developing Balancing Systems to Facilitate the Achievement of Renewable Energy Goals, Position Paper Prepared by WG Renewables and WG Ancillary Services, November 2011.

[7] ñDeterministic frequency deviations ï root causes and proposals for potential solutionsò, a joint EURELECTRIC ï ENTSO-E response paper.

[8] ñIncident Classification Scale Guidelinesò, ENTSO-E, March 2012.

[9] ñNetwork Code ñRequirements for Generatorsò in view of the future European electricity system and the Third Package network codesò, ENTSO-E.

ANNEX 1-DEFINITIONS IN THE FRAMEWORK OF THE OS NC

(N-1)-Criterion means the rule according to which elements within TSOõs Responsibility Area remaining in operation after a Contingency from the Contingency List of the Contingency List of the TSO must be capable of accommodating the new operational situation without exceeding Operational Security Limits; *(definition from OS NC);*

(N-1)-Situation means the situation in the transmission system in which a Contingency from the Contingency List has happened *(definition from OS NC)*;

Active Power - is the real component of the Apparent Power at fundamental Frequency, expressed in watts or multiples thereof (e.g. kilowatts (kW) or megawatts (MW)). (definition from RfG NC)

Active Power Reserve means the Active Power available for maintaining the frequency *(definition from OS NC)*;

Alert State means the operational state where Transmission System is within Operational Security Limits, but a Contingency from the Contingency List has been detected, for which in case of occurrence, the available Remedial Actions are not sufficient to cope with *(definition from OS NC)*;

ancillary services means services necessary to support transmission of electric power between generation and load, maintaining a satisfactory level of operational security and with a satisfactory quality of supply*(definition from Directive 2003/54/EC)*;

Area Control Error (ACE) ï means the sum of the instantaneous difference between the actual and the set-point value (measured total power value and Control Program including Virtual Tie-Lines) for the power interchange of a Control Area, taking into account the effect of the frequency bias for that Control Area which is calculated from the product of the K-Factor and the System Frequency Deviation. (definition from LFC NC)

Blackout State means the state where the operation of part or all of the Transmission System is terminated *(definition from OS NC)*;

Business Continuity Plan means the plan detailing TSOõs responses to a loss of critical tools and facilities *(definition from OS NC)*;;

Common Grid Model (CGM) means the European-wide or multiple-TSOs-wide data set, created by the European Merging Function, through the merging of relevant data *(definition from CACM NC)*;

Connection Point - means the interface at which the Demand Facility, Power Generating Module or interconnector (including HVDC) is connected to a transmission or distribution network, or at which the distribution network is connected to a transmission network as identified in the Connection Agreement (definition from OS NC);

Contingency List means the list of Contingencies to be simulated in the Contingency analysis in order to test the compliance with the Operational Security Limits a priori or a posteriori after a Contingency took place *(definition from OS NC)*;

Contingency means the identified and possible or already occurred Fault of an element within or outside a TSOõs Responsibility Area, including not only the Transmission but also the Distribution Networks of DSOs on lower voltage levels. Internal Contingency is a Contingency within the TSOõs Responsibility Area. External Contingency is a Contingency within the Responsibility Area of neighbouring TSO having effects in the Responsibility Area of the TSO *(definition from OS NC)*;

Critical Fault Clearing Time means the maximum Fault duration for which the electric power system remains transiently stable;

Demand Facility means a facility which consumes electrical energy and is connected at one or more Connection Points, to the exclusion of Distribution Networks and auxiliary supplies of a Power Generating Facility which do not qualify as Demand Facilities (definition from DCC NC);

Distribution Network means the electrical network for the distribution of the electrical power from and to third parties connected to it, a Transmission or another Distribution Network (definition from DCC NC);

Distribution System Operator (DSO) means a natural or legal person responsible for operating, ensuring the maintenance of and developing the distribution system in its Responsibility Area and its interconnections with other systems and for ensuring the long-term ability of the system to meet reasonable demands for distribution of electricity (definition from Directive 2009/72/EC);

Disturbance means an unplanned event that may cause the electric power system to divert from Normal State (definition from OS NC);

Dynamic Stability Assessment (DSA) means the security assessment in terms of Rotor Angle Stability, Frequency Stability and Voltage Stability (definition from OS NC);

Declared Availability means declaration and notice prepared in respect of a Significant Grid User Plant, submitted to the TSO setting out the values and times applicable to those values of availability and ancillary services capability;

Emergency State means the situation where Operational Security Limits are not kept with at least one of the operational parameters outside of the respective limits (definition from OS NC);

ENTSO-E means the European Network of Transmission System Operators for Electricity as established in the Regulation (EC) 714/2009 of the European Parliament and of the Council of 13 July 2009 on conditions for access to the network for cross-border exchanges in electricity and repealing Regulation (EC) 1228/2003[4];

Exceptional Contingency means the unusual ï as opposed to Ordinary Contingency ï loss of one or more elements such as, but not limited to, a double line - two circuits on the same tower over a long distance, where the consideration of distance is left to the determination of the TSO, a single busbar, a circuit breaker failure, a common mode Fault with the loss of more than one Power Generating Facility, a common mode Fault with the loss of more than one DC line (definition from OS NC);

Fault means the event occurring on the primary equipment in the system such as all kinds of short-circuits: single-, double- and triple-phase, with and without earth contact. It means further a broken conductor, open circuit, or an intermittent connection, resulting in a permanent non-availability of the affected Transmission System element *(definition from OS NC);*

Frequency Restoration Controller

Frequency Restoration Control Error means the control error for the Frequency Restoration Process which is equal to the ACE of a LFC Area or is based on the Frequency Deviation where the area geographically corresponds to the Synchronous Area *(definition from OS NC);*

Frequency Stability means the ability of the power system to maintain stable acceptable frequency in N-Situation and after being subjected to a disturbance.

---

4 *OJ L 211, 14.8.2009, p. 15–35*

Isolated System means a system which is designed to operate as a stand-alone system for a definite or indefinite time. It includes systems that bear DC or a single AC interconnection to other synchronous areas.

Load Frequency Control Area (LFC Area) means a part of the Synchronous Area physically demarcated by points of measurement of Tie-Lines to other LFC Areas fulfilling the Area Process Obligations of a LFC Area (definition from OS NC);

Local means the qualification of an Alert, Emergency or Blackout State when there is no risk of extension of the consequences outside of the Transmission System of a single TSO (definition from OS NC);

Normal State means the operational system where the system is within Operational Security Limits in the N-Situation and after the occurrence of any Contingency from the Contingency List, taking into account the effect of the Remedial Actions available; **N-Situation** means the situation where no element of the Transmission System is made unavailable due to a Fault (definition from OS NC);

Observability Area means the area of the relevant parts of the Transmission Systems, relevant DSOs and neighbouring TSOs transmission system, on which TSO shall implement a real-time monitoring and modelling to ensure reliability of the respective Responsibility Area (definition from OS NC);

Operational Security Limits means the acceptable operating boundaries: thermal, voltage, short-circuit current, frequency and stability limits (definition from OS NC);

Operational Security means the Transmission System capability to retain a Normal State or to return to a Normal State as soon and as close as possible, and is characterized by its thermal limits, voltage constraints, short-circuit current, frequency reference value and stability limits (definition from OS NC);

Operational Security Performance Indicators are used for monitoring of the Operational Security; these criteria are based on the definition of Faults, incidents, disturbances and other terms, which influence Operational Security; as specified in the ENTSO-E Incidents Classification Scale according to the Article 8(3)(a) of the Regulation (EC) N°714/2009.

Operational Security Ranking is used for monitoring of the Operational Security on the basis of the Operational Security Criteria, according to the ENTSO-E Incidents Classification Scale according to the Article 8(3)(a) of the Regulation (EC) N°714/2009

Ordinary Contingency means the loss of a Transmission System element such as, but not limited to, a single line, a single Power Generating Facility, a single transformer, a phase-shifting transformer, a voltage compensation installation of 50 MVAr or more or a DC link or a single Demand Facility (definition from OS NC);

Out-of-Range Contingency means the very unusual simultaneous loss of several Transmission System elements such as, but not limited to two independent lines, a substation of more than one busbar, a tower with more than two circuits or a power swinging or oscillation event leading to the loss of more than one large Power Generating Facility (definition from OS NC);

Power Generating Facility means a facility to convert primary energy to electrical energy which consists of one or more Power Generating Modules connected to a Transmission or Distribution Network at one or more Connection Points (definition from RfG NC);

Power Generating Module means is either a Synchronous Power Generating Module or a Power Park Module (definition from RfG NC);

Power Generating Facility Operator means the natural or legal person which is the operator a Power Generating Facility (definition from OS NC);

Ramping Rate means the rate of change of active power by a Power Generating Module, Demand Facility or DC interconnection (definition from OS NC);

Redispatching means a measure activated by one or several System Operators by altering the generation and/ or load pattern, in order to change physical flows in the grid and relieve a physical congestion; (definition from CACM NC)

Remedial Action means a measure activated by one or several System Operators, manually or automatically, that relieves or contributes to relieving Physical Congestions. They can be applied prefault or post-fault and may involve costs (definition from CACM NC);

Reactive Power - is the imaginary component of the Apparent Power at fundamental Frequency, usually expressed in kilovar (kvar) or megavar (Mvar). (definition from RfG NC)

Reactive Power Reserve means the Reactive Power which is available for maintaining the voltage (definition from OS NC);

Regional Security Coordination Initiative (RSCI)- means regional unified scheme set up by TSOs in order to coordinate Operational Security analysis on a determined geographic area (definition from OPS NC);

Responsibility Area means a coherent part of the interconnected system operated by a single TSO with physical loads and/ or generation units connected within the area, if any (definition from OS NC);

Restoration means the state where the objective is to re-establish the system after a Blackout (definition from OS NC);

Schedule means the reference set of values of energy or power within a future time period and for a resolution time interval (definition from OPS NC);

Security Plan means the plan containing a risk assessment of critical TSOqs assets to major physical- and cyber-threat scenarios with an assessment of the potential impacts (definition from OS NC);

Set-Point means the target value for any parameter typically used in control schemes (definition from OS NC);

Significant Grid User means the pre-existing system users and new system users which are deemed significant on the basis of their impact on the cross border system performances via influence on the LFC Areaqs security of supply including provision of ancillary services (definition from OS NC;

Stability Limits means the permitted operating boundaries of the Transmission System in terms of respecting the constraints of Voltage Stability, Rotor Angle Stability and Frequency Stability (definition from OS NC) ;

State Estimation means the methodology and algorithms used to calculate a reliable set of measurements defining the state of the Transmission System out of the redundant set of measurements which might contain faulty and inaccurate values or where some measurement values are missing (definition from OS NC);

Synchronous Area means an area covered by interconnected TSOs with a common system frequency in a steady operational state. The following Synchronous Areas are covered in this NC: Continental Europe (CE), Cyprus (CY), Great Britain (GB), Iceland (ICE), Ireland (IRE) and Northern Europe (NE) (definition from LFC NC);

System Frequency - Number of instantaneous oscillations of alternating current in a power system per time interval given in [Hz] (definition from LFC NC);

System Defence Plan means the summary of all technical and organisational measures to be undertaken to prevent the propagation or deterioration of an incident in the Transmission System, in order to avoid a widespread disturbance and Blackout State (definition from OS NC);

System Protection Schemes (SyPS) means the set of coordinated and automatic measures designed to ensure fast reaction to disturbances and to avoid their propagation in the transmission system. SyPS can include event or measure based and may use telecommunication infrastructure to transmit the activation measures (definition from OS NC);

System Operator Employee means the person in charge of operational control of the transmission system in real-time (definition from OS NC);

System State means the operational state of the transmission system in relation to the Operational Security Limits, namely: Normal, Alert, Emergency, Blackout and Restoration (definition from OS NC);

system user means the natural or legal person supplying active and/or reactive power to a TSO or DSO grid, or being supplied with active and/or reactive power from a TSO or DSO grid(definition from the Directive *2003/54/EC*);

Transitory Admissible Overloads means the temporary overloads of Transmission System elements or secondary equipment which are allowed for a limited period and which do not cause physical damage to the elements or secondary equipment as long as the defined duration and thresholds are respected (definition from OS NC);

Transmission System means the electric power network used to transmit electric power over long distances within and between Member States. The Transmission System is usually operated at the 220 kV and above for AC or HVDC, but may also include lower voltages (definition from CACM NC);

Voltage Control means the balancing of the reactive power needs of the network and the Grid Users in order to maintain permitted voltage profile (definition from OS NC);

Voltage Stability means the ability of a transmission system to maintain acceptable voltages at all buses in the electric power system under N-Situation and after being subjected to a disturbance (definition from OS NC);

WIDE AREA means the qualification of an Alert, Emergency or Blackout State when there is a risk of propagation to the interconnected Transmission Systems (definition from OS NC).