Operational Security Network Code

4th Workshop

20. December 2012

entsoe

Reliable Sustainable Connected

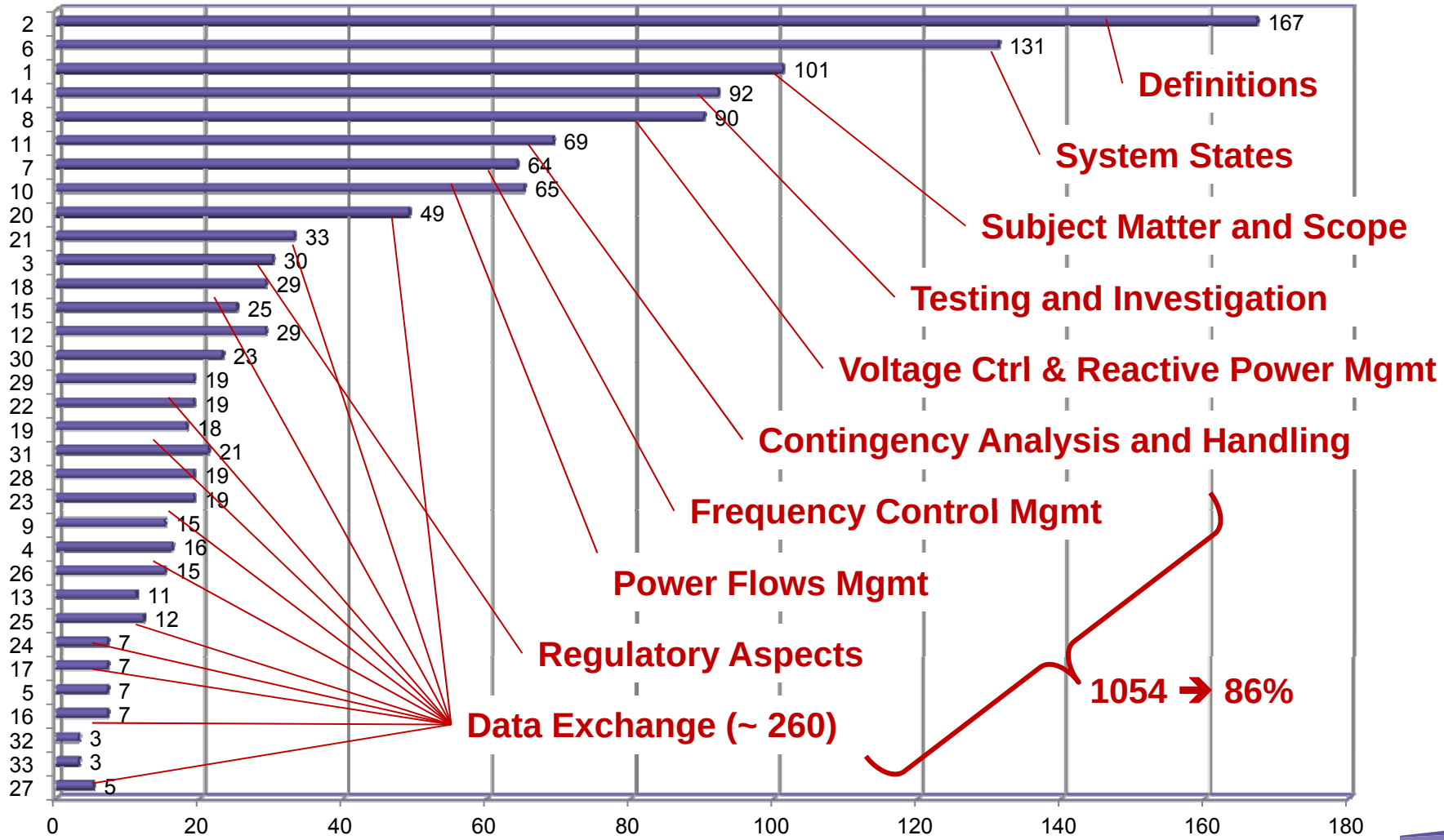
Agenda

- **Summary of OS NC Public Consultation**
- **Overview of Key Issues – summary**
- **Key Legal Issues**
- **OS NC Articles & amendments - details**

Agenda

- **Summary of OS NC Public Consultation**
- **Overview of Key Issues – summary**
- **Key Legal Issues**
- **OS NC Articles & amendments - details**

Statistics: number of comments per article



Agenda

- Summary of OS NC Public Consultation
- **Overview of Key Issues – summary**
- Key Legal Issues
- OS NC Articles & amendments - details

Key Issues: NRA involvement

- **Approach: consultation of TSO and/or DSO with its NRA, to establish terms, conditions or actions necessary for Operational Security**
  - Article 1 and Article 2: Definition and significance test for Significant Grid Users
  - Article 6(16): Business Continuity Plan about critical tools & facilities
  - Article 6(17): Security Plan about critical infrastructure (CIP …)
  - Article 7(4): Power Generating Modules frequencies and duration of withstanding disconnection
  - Article 7(15): Definition restrictions of active power Ramping Rates for all kinds of reserves

Key issues: NRA involvement *(cont'd)*

- Article 8(3): Power Generating Modules voltages and duration of withstanding disconnection
- Article 8(14): definition of reactive power set-points or power factor angles to be maintained by Grid Users at the Connection Points
- Article 8(17): definition and coordination of Voltage Control actions with Significant Grid Users, directly connected DSOs and neighbouring TSOs
- Article 9(1): max./min. short circuit current
- Article 10(1): Operational Security Limits for power flows on all transmission network elements including interconnections

Key issues: NRA involvement *(cont'd)*

- Articles 10(5) and 10(6): Redispatch measures
- Article 11(16): defining the applicable, most restrictive Operational Security Limits at the interconnections
- Article 12(7): definition of underfrequency demand disconnection measures and overfrequency measures
- Article 13(4): dynamic stability measures (PSS) infolving Power Generating Modules which are Significant Grid User
- Article 13(5): determining the minimum intertia to be procured in a market based way, required for system stability

Key issues: NRA involvement *(cont'd)*

- Articles 14 to 27 (Data Exchange): coherent contents, timestamping and periodicity of data reporting, data from directly connected DSOs, additional data from Power Generating Facility Operators, …
- Article 30: Operational Security Performance Indicators ➔ see next …
- Article 30(11): definition of priority users in terms of disconnection and reenergizing (e.g. nuclear plants)

Key issues: Operational Security Performance Indicators

Articles 2, 30(2), 30(3): Operational Security Performance Indicators & Ranking

Article 30(1)(a): means within own Responsibility Area: real-time operation, operational planning, disturbances prevention / remedy

Article 30(1)(b): means through cooperation with other stakeholders: redispatch, congestion mgmt., reserves, ancillary services

Based on findings from annual ICS reporting:

Article 30(1)(c): enhancements within own Responsibility Area

Article 30(1)(d): new means involving other stakeholders

Key issues: Operational Security Performance Indicators *(cont'd)*

Criteria Definition from ICS:

- Number of tripped transmission system elements;
- Energy [MWh] of disconnected Generation Facilities per year;
- Energy [MWh] of disconnected Demand facilities per year;
- Time of being in Operational States other than Normal State (Alert, Emergency, Blackout);
- Duration times within which there was a lack of reserves identified;
- Voltage deviation;
- Frequency deviation per Synchronous Area;
- Number of system-split separations and / or local blackouts;
- Number of regional blackouts involving two or more TSOs;
- Explanation of reasons of incidents at the levels 2 and 3

Key issues: Operational Security Performance Indicators *(cont'd)*

Ranking Definition from ICS:

- Level 0: normal operation of the transmission system - Normal State (no reporting)
- Level 1: alert operation of the transmission system - Alert State
- Level 2: emergency operation of the transmission system - Emergency State
- Level 3: blackout of the transmission system - Blackout State

Key issues: Operational Security Performance Indicators *(cont'd)*

„Draft sample annual report 01-03/2012" *for illustration*

	Level 1	Level 2	Level 3
Number of tripped grid equipment, leading to overload, violation of N-1, limitation of transfer capacity	79	0	N/A
Disconnected generation per year, MWh	0 MMh	0 MWh	N/A
Disconnected load per year, MWh	0 MWh	0 MWh	0 MWh
Time of being in different states (alert, emergency, black-out), h	267 h	0 h	0 h
Time of lack of reserves (> 20%), h	92 h	N/A	N/A
Voltage deviation	0	N/A	N/A
Frequency deviation (frequency curves of the different synchronous areas)	2	0	0
Number of separation of the system and/or local black-outs (1 TSO)	N/A	0	N/A
Number of regional black-outs	N/A	N/A	0

Key issues: frequency & voltage

- **Cross-references and justification in relation to the RfG NC provisions at Connection Point**
- **Article 7 Frequency Control Management**
  - TSOs‘ compliance with the frequency quality parameters (LFC&R) & back to max. steady state deviation ASAP between 49-51 Hz
  - Best endeavour & system defence for freq. restoration outside above & Grid Users obligation according to RfG (frequencies & times)
- **Article 8 Voltage Control and Reactive Power Mgmt.**
  - Voltage at Connection Point cf RfG & restoration back within time ranges from Articles 11 RfG and 14 DCC
  - Coordinate at Synchronous Area level

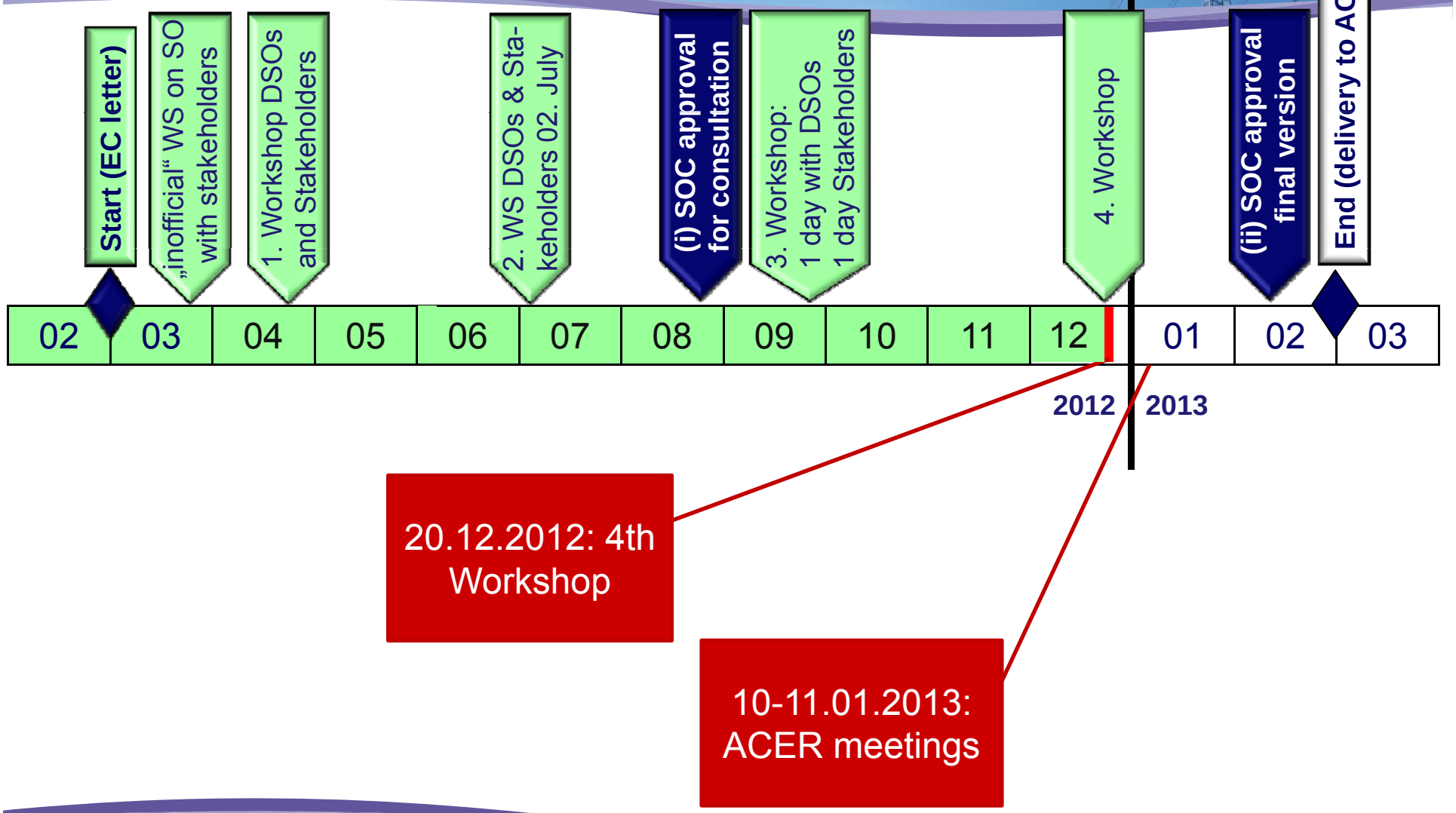
Further issues & amendments

- Coordination of Remedial Actions or a System Defence Plan with consequences on directly connected DSOs, with DSOs and Significant Grid Users (Art. 6(10))
- Clarity / explanation on issues like e.g. frequency plan, contingency analysis, etc. (i.e. no worsening)
- Common Grid Model ← reference from OPS NC
- Avoiding redundancies in data exchange and contingency analysis (Art. 11(14))

Further issues & amendments (cont‘d)

- **Significance test for the „Significant Grid Users“**
  - Introduced, further explanation / examples into Supporting Paper
- **Merged Testing and Investigation into Compliance**
- **Annex with ICS …**

Roadmap & next steps



Agenda

- Summary of OS NC Public Consultation
- Overview of Key Issues – summary
- **Key Legal Issues**
- OS NC Articles & amendments - details

NC OS: Key legal issues

- **Article 1(2): Isolated systems (exemption of Balearic Islands)**
- **Article 1(3): Significant Grid User (specific definition)**
- **Article 3(3): Generic clause (NRA involvement; meeting with ACER lawyers 08.01.2013)**
- **Article 4(4): Cost recovery**
  - TSOs / DSOs in cooperation with NRA shall develop methodology
  - Reasonable costs of other than compliance tests to be borne by requestor
- **Article 33: Entry into force within 2 years period**

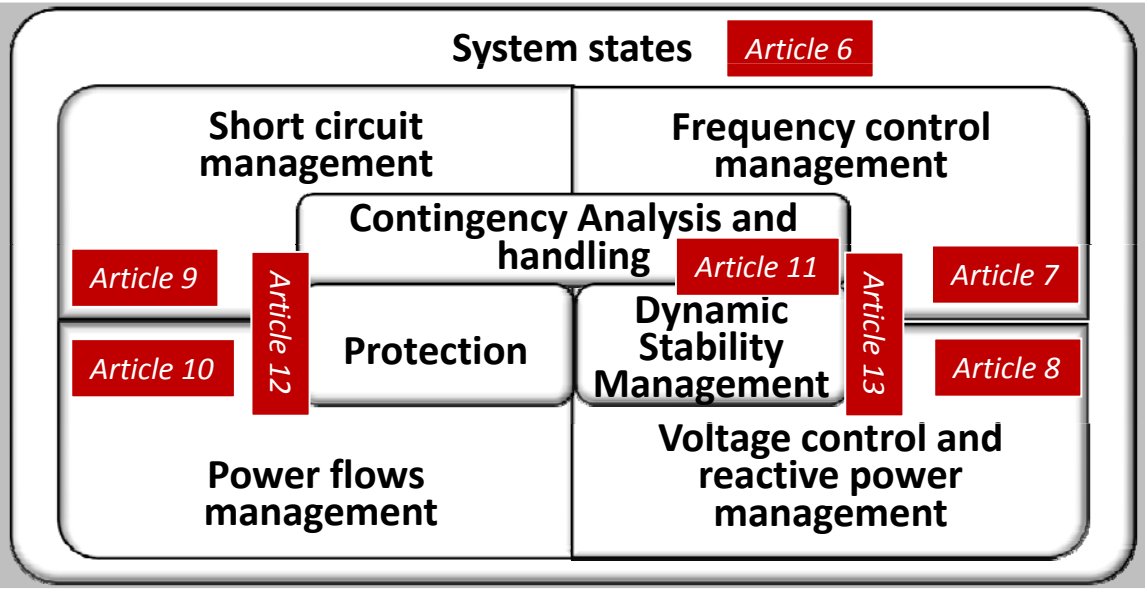
Agenda

- Summary of OS NC Public Consultation
- Overview of Key Issues – summary
- Key Legal Issues
- **OS NC Articles & amendments - details**

OS NC final structure and contents

1. General provisions: Subject matter and scope, Definitions, Regulatory aspects, Recovery of costs, Confidentiality obligations — *Articles 1-5*

2. Requirements



3. Data exchange — Data exchange — *Articles 14-27*

4. Training — Operational training and certification — *Article 28*

5. Compliance — Responsibilities, Testing, Analysis (incl. PI) — *Articles 29-31*

6. Final provisions — *Articles 32-33*

Annex I Incidents Classification Scale

Chapter 1 General provisions

1. General provisions: Subject matter and scope, Definitions, Regulatory aspects, Recovery of costs, Confidentiality obligations — *Articles 1-5*

2. Requirements

- System states — *Article 6*
- Short circuit management — *Article 9*
- Frequency control management — *Article 7*
- Contingency Analysis and handling — *Article 11*
- Protection — *Article 10*, *Article 12*
- Dynamic Stability Management — *Article 13*, *Article 8*
- Power flows management
- Voltage control and reactive power management

3. Data exchange — Data exchange — *Articles 14-27*

4. Training — Operational training and certification — *Article 28*

5. Compliance — Responsibilities, Testing, Analysis (incl. PI) — *Articles 29-31*

6. Final provisions — *Articles 32-33*

Annex I Incidents Classification Scale

Article 1 Subject matter and scope

- **Art. 1(1): (Operational Security Network Code as the ‚umbrella' for the System Operation Codes**
  - OS NC sets the overall principles
  - Reflects on the common issues for LFC&R and OPS NC (Emergency …)
- **Art. 1(3): Significant Grid Users**
  - New definition and significance test
- **Art. 1(5): clear focus on human and nuclear safety (no ‚other related provisions' …)**

Article 2 Definitions

- **Connection Point and Operational Security defined specially for the OS NC**
- **A number of new / adjusted definitions in order to be consistent and coherent with all other Network Codes**
- **Operational Security Performance Indicators & Ranking**

Article 3 Regulatory aspects & Article 4 Recovery of costs

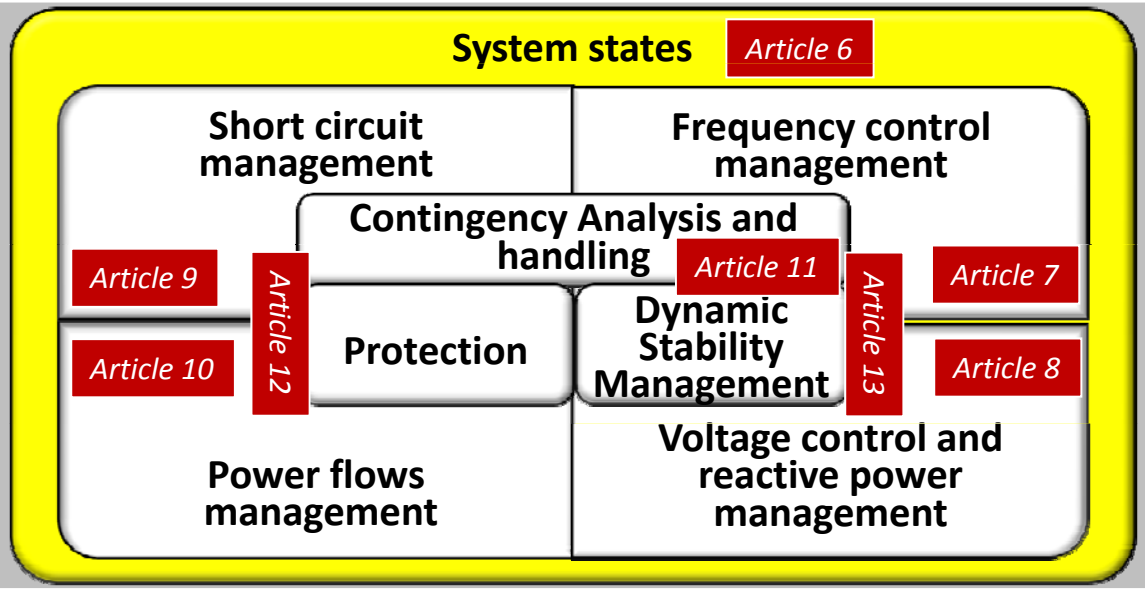
- **Art. 3(3): adjusted and more precise formulation**
- **Art. 3(5): clarification on nuclear power plants**

- **Art. 4(4): TSOs / DSOs (while respecting provisions of Art. 3(3)), in cooperation with NRAs, to develop the methodology for recovering the costs of testing the compliance with the OS NC**

Article 6 System states

1. General provisions: Subject matter and scope, Definitions, Regulatory aspects, Recovery of costs, Confidentiality obligations — *Articles 1-5*

2. Requirements



3. Data exchange — Data exchange — *Articles 14-27*

4. Training — Operational training and certification — *Article 28*

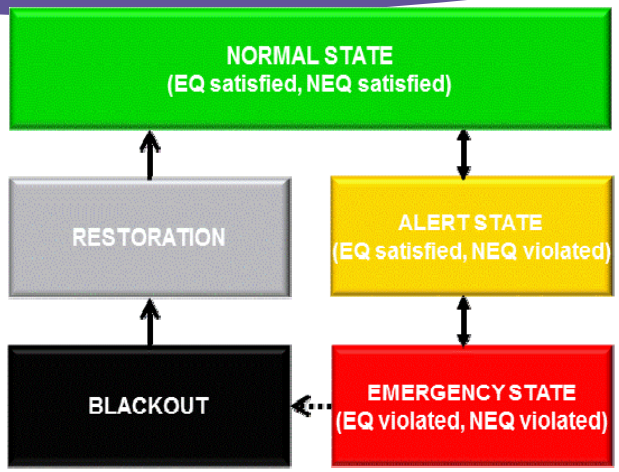
5. Compliance — Responsibilities, Testing, Analysis (incl. PI) — *Articles 29-31*

6. Final provisions — *Articles 32-33*

Annex I Incidents Classification Scale

Article 6 System states *(cont'd)*

- Criteria for system states
- Monitoring the system state
- Information / awareness system
- Operational Security Limits
- Preparation and implementation of remedial actions
- Business continuity plan
- Security plan
- Security Analysis



EQ=Equality contraints (e.g. generation/demand balance)
NEQ = inequality constraints (e.g. voltage thresholds, (n-1)-violations)

Article 6 System states *(cont'd)*

130 comments on this article ; main themes emerging several times :

- Need for more common principles and values to define system states
- Consequences of the system states for grid users ; actions to be done in each state
- Monitoring of alert/emergency states, and transparency
- Priority in re-energizing process
- Need for more figures and more obligations for TSOs
- Links with frequency and voltage ranges defined in RfG and DCC NC
- Stakeholders and NRA involvement in the definition of Operational Security Limit
- PGF involvement in coordination ; DSOs involvement in coordination
- Links with contractual agreements in place
- Cost recovering for SGU participating in a remedial action
- Definition of SGU to be clarified
- Links and consistency with OPS NC and CACM NC

Article 6 System states *(cont'd)*

Main changes to the code in link with these comments :

- More figures and more precise engagements for TSOs in Articles 6, 7, 8 and 10
- Consistency with SGU capabilities defined in RfG NC, DCC NC or National Laws
- Definition of Significant grid users has been added in article 1
- Articles 1(5), 3(5) and 31(11) : respect of relevant provisions for human security, nuclear safety ; and list of high priority system users
- Article 30 describes TSO's responsibilities ; and annual reporting from TSOs
- Coordination : more precision and differentiation between "before real-time" and "implementation in real-time"
- Reference to article 3(3) has been added when NRA involvement is needed

The position paper will answer the comments regarding:

- consequences of the system states for grid users
- stakeholders and NRA involvement in the definition of Operational Security Limit

Articles 6(1) to 6(4) : Criteria for system states

•The article gives precise criteria to characterize the state of the system in a coherent way in every part of the grid ; Articles 7 and 8 contains more precise figures for operational security limits for voltage and frequency, and article 11 gives common principles regarding contingencies to take into account for system state assessment.

•Threshold for estimation of reserve lacks and for declaring a blackout state in line with criteria of the Incident Classification Scale

•The supporting paper will explain that in alert state the system is secure in N situation, so there is no direct consequence for grid users ; a precise definition of the impact on grid users in case of emergency state can't be done in the code, since it can be very different depending of the succession of events that have occurred on the system.

•Content of system defense actions and plan, coordination in emergency and restoration processes will be described in the emergency NC

Articles 6(1) to 6(4) : Criteria for system states

•Articles 7 and 8 will give more figures and obligations for TSOS, defining more precisely thresholds for voltage and frequency, and contingencies to take into account in security analysis. TSOs are not the only body who influences the parameters of the system, so they can do their best but cannot guarantee normal state in all circumstances.

•TSOs need to know system capabilities in real-time so the availability of reserves is important to evaluate e.g. available remedial actions ; definition of reactive Power Reserve has been added in the article 2

Articles 6(6) to 6(8) : Information / awareness system

•Alert state doesn't have any consequence on grid user and the probability that the alert state degrades to achieve a state of emergency may be quite low. Alerting grid users at every alert could be harmful because warning could lose credibility

•Transparency is market issue and dealt within EU transparency guidelines. Not all information should be open close to real time.

•The first priority is to recover the system as fast as possible, so information will be delivered first to those who are involved in restoration plan. Further steps in communication and coordination in case of blackout state will be defined in Emergency NC.

Articles 6(9) to 6(14) : remedial actions

•Coordination has to be prepared ex-ante, so that the remedial actions can be set up quickly as soon as the state of the system requires.

•The new version of the NC deals with the preparation phase and the implementation phase in two different articles. DSOs shall be part of the coordination ex-ante, so as the remedial actions can be validated before real time and set up without discussion when needed in real-time

•The NC defines the needs for secure operational conditions of the system; contractual agreements shall be in line with the requirements of the code, otherwise they must be adapted. Of course the code complies with connection codes and nuclear safety issues.

•In accordance with the Incident Classification Scale, the number of alert or emergency states will be counted and the evolution of their number will be analyzed.

Article 6(5) : Operational Security Limits

- Explicit link with capabilities defined in both RfG NC, DCC NC and National grid Codes has been added. Article 8 now gives figures for voltage ranges. The following sentence has been added :

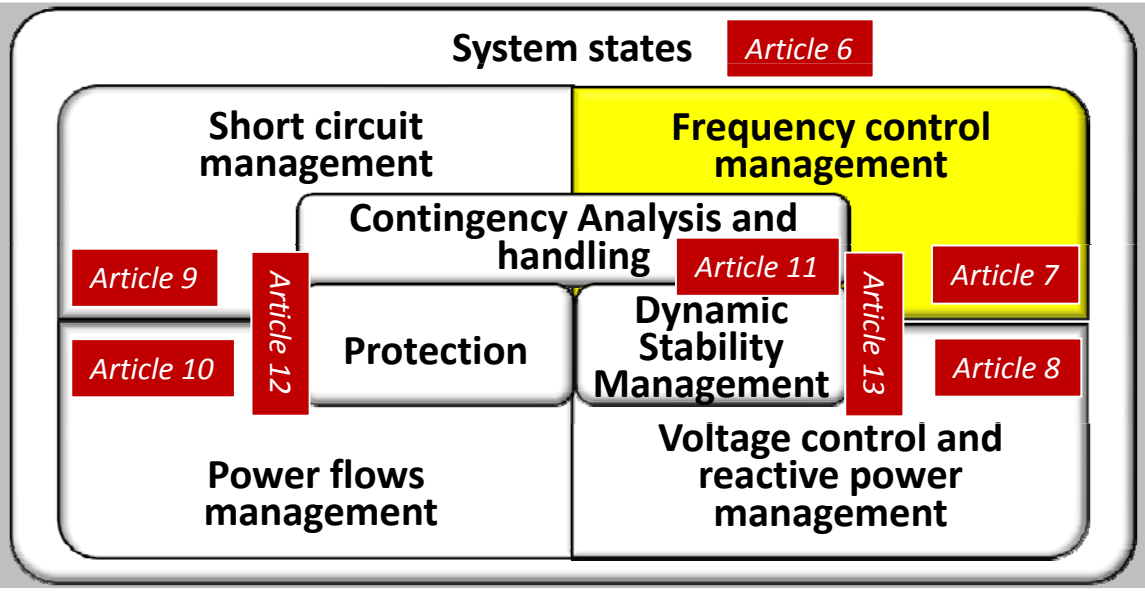
- “When defining these Operational Security Limits, each TSO shall take into account the capabilities required for Grid Users in [NC RfG] and [NC DCC] and national grid codes, in order that voltage and frequency ranges in Normal and Alert States do not lead to their disconnection”

- NRA should be informed, but security limits are defined according to characteristics of equipment by TSOs.

Article 7 Frequency control management

1. General provisions: Subject matter and scope, Definitions, Regulatory aspects, Recovery of costs, Confidentiality obligations — *Articles 1-5*

2. Requirements



3. Data exchange — Data exchange — *Articles 14-27*

4. Training — Operational training and certification — *Article 28*

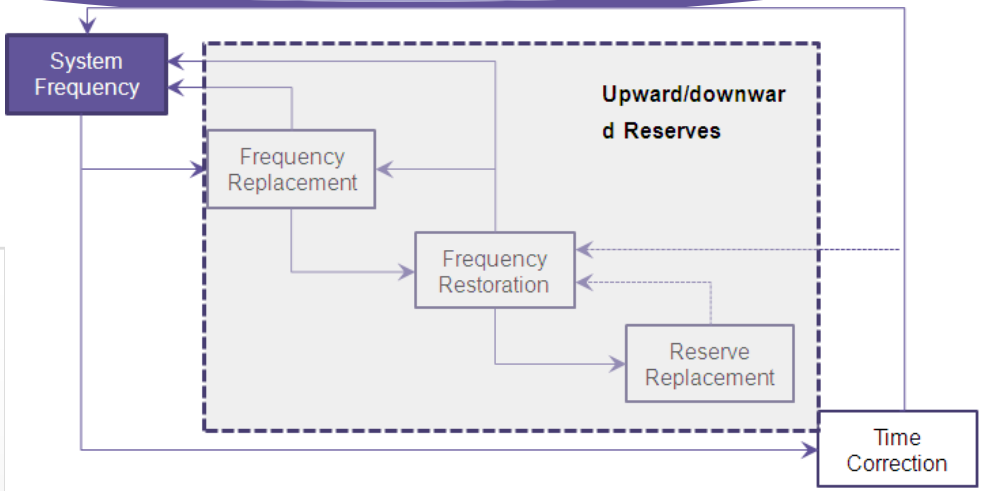
5. Compliance — Responsibilities, Testing, Analysis (incl. PI) — *Articles 29-31*

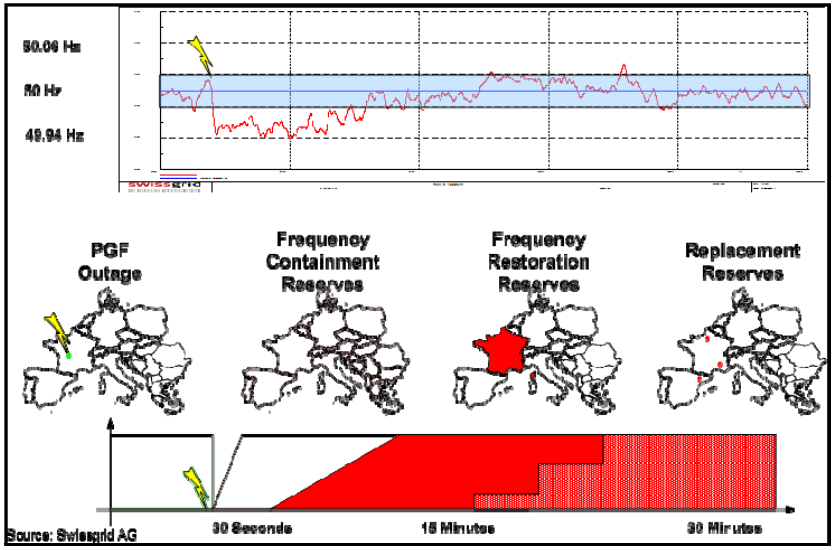
6. Final provisions — *Articles 32-33*

Annex I Incidents Classification Scale

Article 7 Frequency control management *(cont'd)*

- Synchronous Area approach
- „Umbrella" provisions – detailed provisions in [NC LFC&R]
- Continuous Frequency Monitoring
- Frequency quality criteria
- Definition and coordination of System Defence Plan measures
- Provision and activation of active power reserves





Article 7 Frequency control management *(cont'd)*

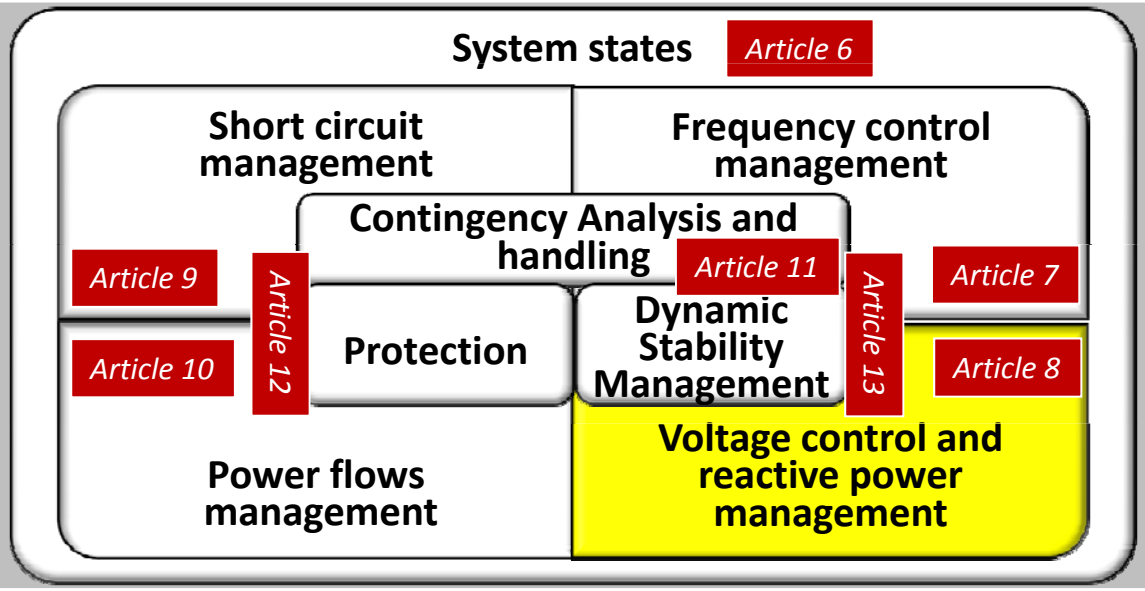
Main changes in conjuction with these comments :

- Specific figures introduced in Article 7(1)
- Frequency ranges and provisions harmonized with [NC RfG] and [NC DCC]
- Distinction between existing and new Significant Grid Users introduced
- System Defence measures in cases of frequency excursions harmonized at least on a Synchronous Area level
- Coordination among TSOs, DSOs and Significant Grid Users enhanced
- Provision on Ramping Rates included
- Provision on High Priority Customer included
- The **Position Paper** together with **Incident Classification Scale (ICS)** further elaborate on the frequency quality monitoring processes.

Article 8 Voltage control and reactive power management

1. General provisions: Subject matter and scope, Definitions, Regulatory aspects, Recovery of costs, Confidentiality obligations — *Articles 1-5*

2. Requirements



3. Data exchange — Data exchange — *Articles 14-27*

4. Training — Operational training and certification — *Article 28*

5. Compliance — Responsibilities, Testing, Analysis (incl. PI) — *Articles 29-31*

6. Final provisions — *Articles 32-33*

Annex I Incidents Classification Scale

Article 8 Voltage ctrl & reactive power mgmt. *(cont'd)*

Ensure that:

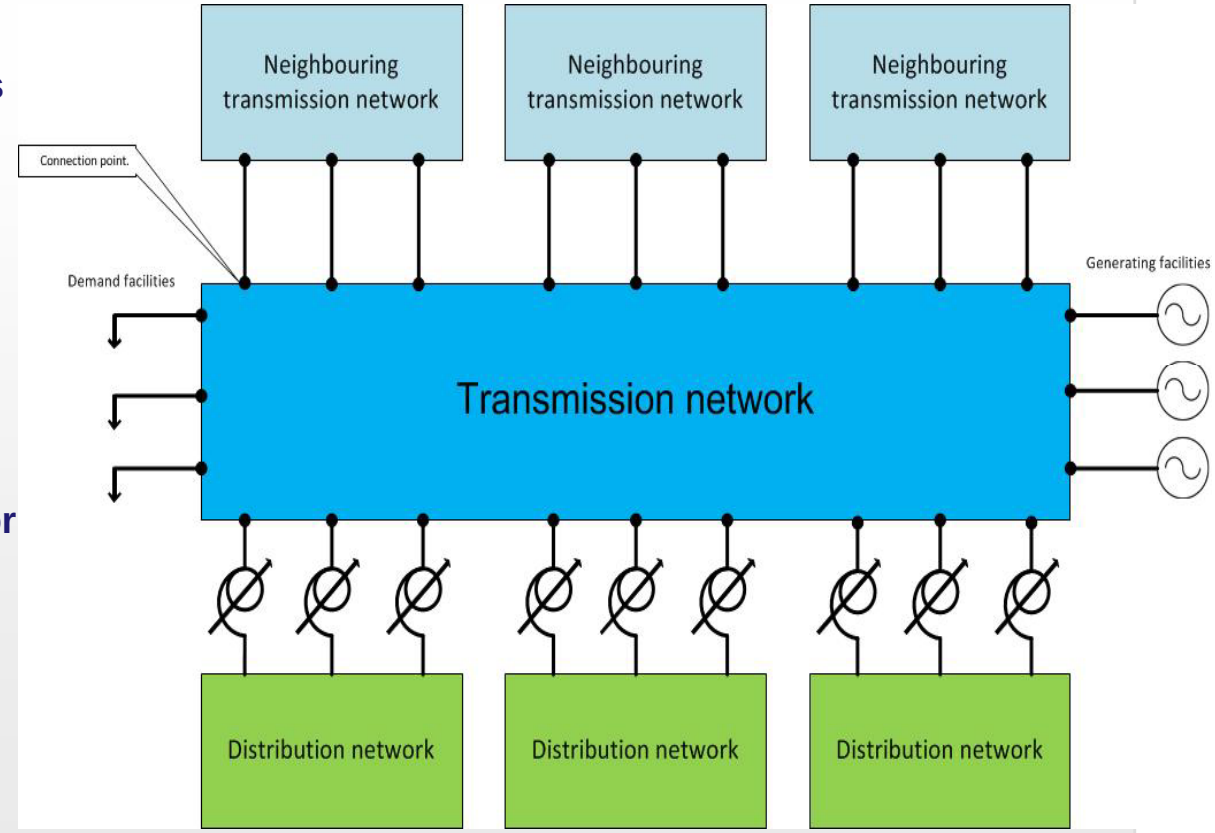
- Voltage levels, reactive power flows, and reactive power resources are monitored, controlled, and maintained within limits
- Voltage Stability of the Transmission System is maintained.
- Remedial actions are prepared to cope with identified violations of the voltage operational security limits.
- TSOs coordinate voltage control actions

in order to:

- Protect equipment and secure operation of interconnected power system.
- Maintain Voltage Stability of the Transmission System
- Prevent a contrary effects to the Operational Security which might be caused by individual actions of TSOs or DSOs

Article 8 Voltage ctrl & reactive power mgmt. *(cont'd)*

- **Monitor, control and maintain in real time voltage levels and reactive power flows**
- **Set voltage and reactive power limits at Connection Points**
- **Prepare and coordinate remedial actions to cope with violations of operational security limits.**
- **In case of voltage deterioration may direct DSOs and Grid Users to block automatic voltage/reactive power control of transformers and/or may have to disconnect Customers and/or Generating Facilities to avoid jeopardising the transmission system.**
- **Providers of reactive power reserve to the TSO shall provide to the TSO information on their available reactive power reserve**



Article 8 Voltage ctrl & reactive power mgmt. *(cont'd)*

90 comments were received on this Article. Most of the comments addressed the following points:

- 4 (voltage limits at the connection point)
- 6 (disconnection at the specified voltages)
- 5 (remaining connected of power generating facilities) ,
- 12 (maintaining voltage and reactive power flows at interconnection points by TSOs and DSOs),
- 7 (using of all available reactive power resources)
- 8 (preparing Remedial Actions),
- 9 (monitoring of respecting of operational voltage limits) ,
- 1 (maintaining the voltage and reactive power flows).

The rest of comments proposed new paragraphs related mainly to the issue of registration of occurrences of voltages outside ranges in 8.1.
Many comments have been repeated by different commenters what suggest that answers were coordinated between them.

Article 8 Voltage ctrl & reactive power mgmt. *(cont'd)*

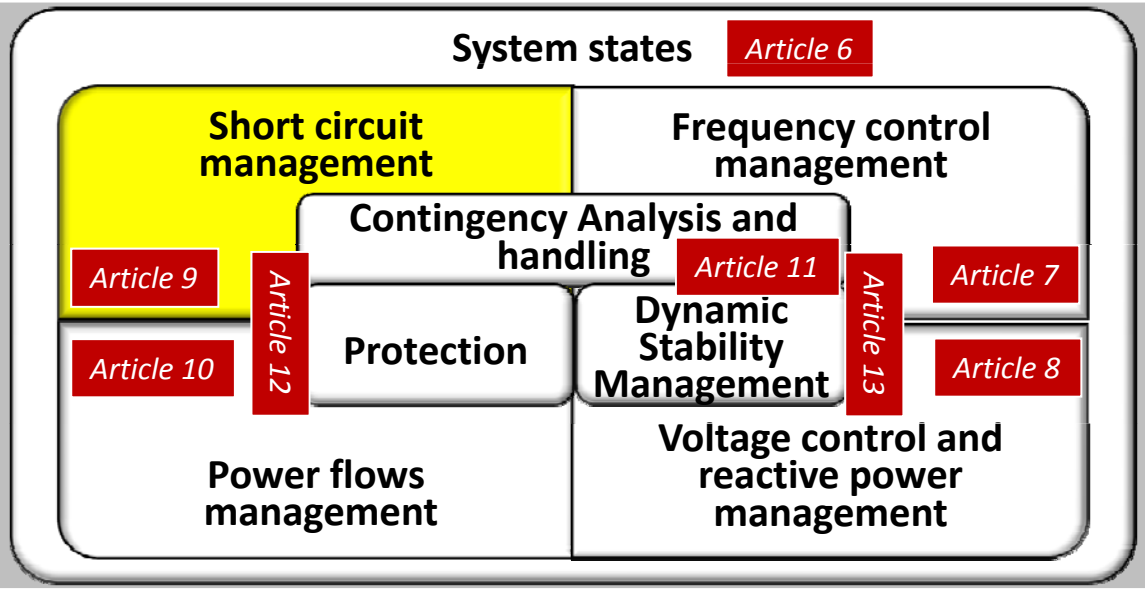
Main amendments introduced:

- Better and more precise formulation of requirements
- Specific voltage figures
- Requirements in case of voltages outside normal voltage ranges
- More precise formulation for requirements for disconnection from the grid
- Consistency with other NCs and references to other NCs

Article 9 Short circuit management

1. General provisions: Subject matter and scope, Definitions, Regulatory aspects, Recovery of costs, Confidentiality obligations — *Articles 1-5*

2. Requirements



3. Data exchange — Data exchange — *Articles 14-27*

4. Training — Operational training and certification — *Article 28*

5. Compliance — Responsibilities, Testing, Analysis (incl. PI) — *Articles 29-31*

6. Final provisions — *Articles 32-33*

Annex I Incidents Classification Scale

Article 9 Short circuit management

***Short Circuit Management* serves to calculate short circuit currents within and beyond the borders of the Control Area, ensuring adequate treatment of short circuit Faults.**

Keeping the impact of short-circuit currents at a secure level of functioning of the Transmission System implies:

- Enabling accurate short-circuit current calculation by TSOs.
- Monitoring the short-circuit currents, applying remedial actions in case of violation of OS Limits.
- Provision of information and communication to affected TSOs, DSOs and Significant Grid Users => be able to consider the effect of other Transmission and Distribution systems.

Article 9 Short circuit management *(cont'd)*

- 15 comments were received on this Article.

- Four themes emerged several times:
  - NRA involvement.
  - Distinction between the terms Control Area, Observability Area and Responsibility Area
  - Minimum limits of short-circuit current.

- Several remarks were repeated by different stakeholders => concerned answers have been coordinated while evaluating those comments

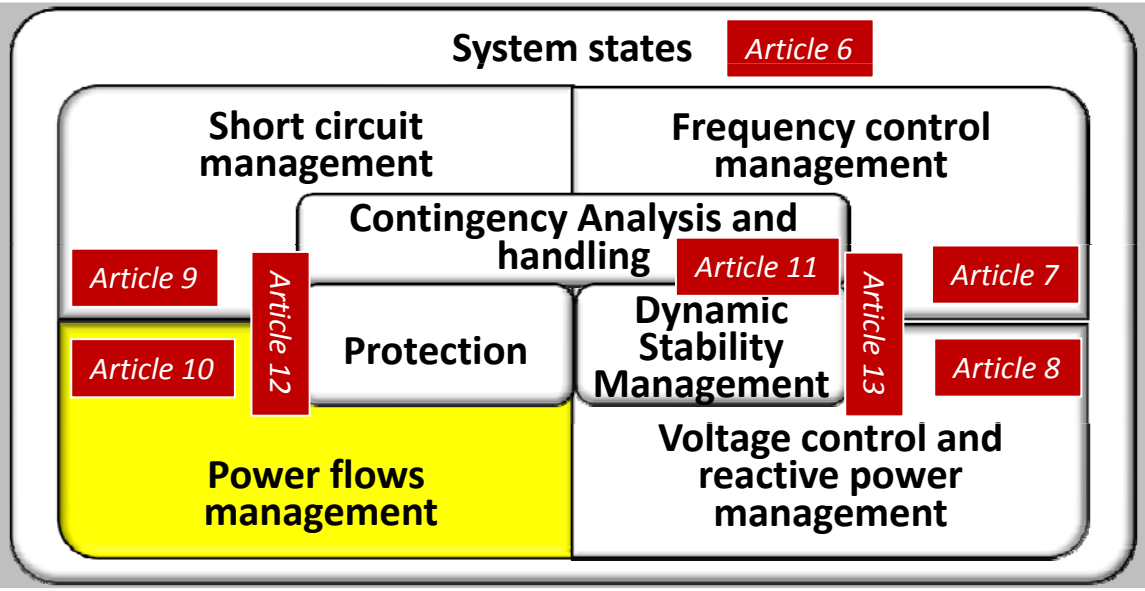
Article 9 Short circuit management *(cont'd)*

- Reference of operation according to national safety legislation has been added in Article 9.1, because Articles 5 and 12 of the Directive 2009/72 do not directly impose a strict obligation to TSOs to ensure the short circuit management.
- Reference to Article 3(3) has been added in Article 9(2) and definition of minimum (and not only maximum) limits of admissible short-circuit current by the TSO.
- OS NC establishes a harmonised framework for short-circuit current calculation in Article 9(3). The aim is not to rewrite in detail existing IEC standards.
- The term "Observability Area Network" leads to confusion with the term "Observability Area" and does not add any additional value to the requirement.

Article 10 Power flows management

1. General provisions: Subject matter and scope, Definitions, Regulatory aspects, Recovery of costs, Confidentiality obligations — *Articles 1-5*

2. Requirements



3. Data exchange — Data exchange — *Articles 14-27*

4. Training — Operational training and certification — *Article 28*

5. Compliance — Responsibilities, Testing, Analysis (incl. PI) — *Articles 29-31*

6. Final provisions — *Articles 32-33*

Annex I Incidents Classification Scale

Article 10 Power flows management *(cont'd)*

Objectives

- Maintain power flows below operational power flow limits in every element of the transmission grid to:
  - Protect people in the vicinity and equipment of the installations.
  - Avoid cascading effect and spreading of incidents.
- Provide the means to perform efficient analysis and monitor power flow levels in responsibility area.
- Prepare remedial actions to avoid violations of the operational security limits.
- Coordinate remedial actions with neighbouring TSOs

Article 10 Power flows management *(cont'd)*

63 comments were received on Article 10 "Power Flow Management". These were the main issues raised:

- NRA involvement
- Definition of the Operational Security Limits
- Coordination with other Distributors and Significant Grid Users
- Redispatch meassures

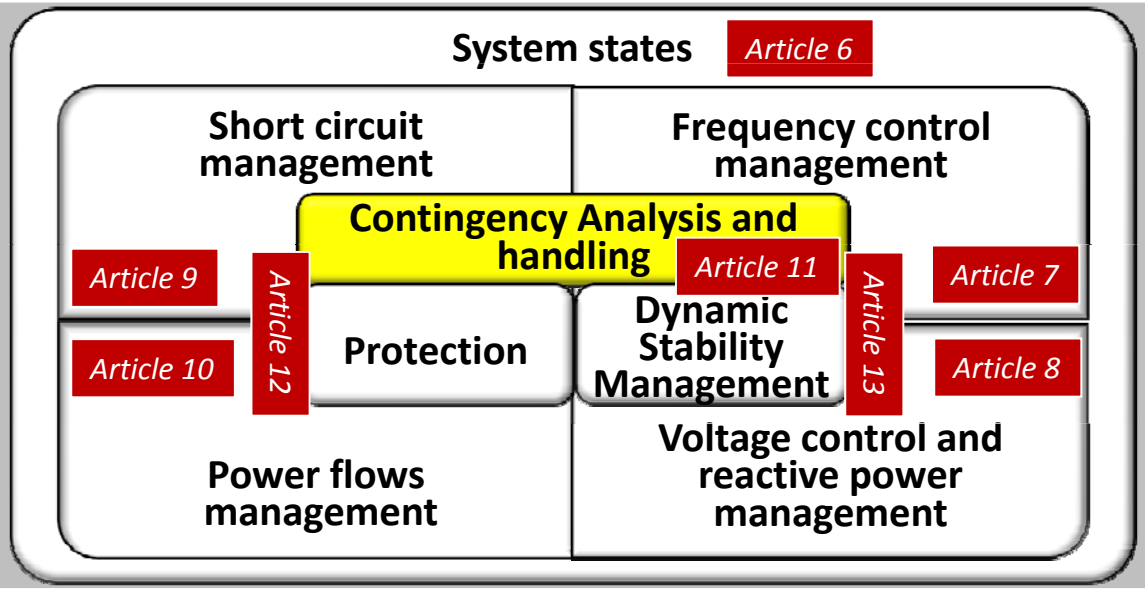
Some other comments were made to improve the understanding of the code.

Some paragraphs were rewritten to achieve a better formulation and It has been made reference to NRA involvement in paragraphs related to the definition of the OSL and Redispatching.

Article 11 Contingency analysis and handling

1. General provisions: Subject matter and scope, Definitions, Regulatory aspects, Recovery of costs, Confidentiality obligations — *Articles 1-5*

2. Requirements



3. Data exchange — Data exchange — *Articles 14-27*

4. Training — Operational training and certification — *Article 28*

5. Compliance — Responsibilities, Testing, Analysis (incl. PI) — *Articles 29-31*

6. Final provisions — *Articles 32-33*

Annex I Incidents Classification Scale

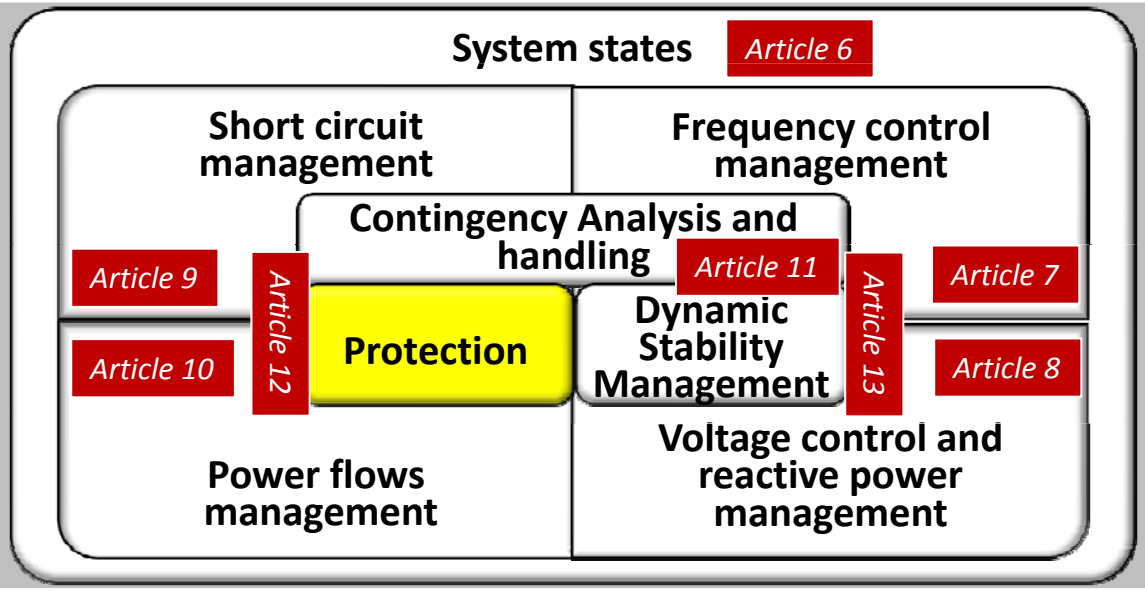
Article 11 Contingency analysis and handling *(cont'd)*

- **Art. 11(1): Ordinary and optionally Exceptional Contingencies to be included in the Contingency List**
- **Art. 11(5)(d): Clarification, simplification and shortening**
- **Art. 11(10): Refer to the responsible national authority (possible differences among the MS …)**

Article 12 Protection

1. General provisions: Subject matter and scope, Definitions, Regulatory aspects, Recovery of costs, Confidentiality obligations — *Articles 1-5*

2. Requirements



3. Data exchange — Data exchange — *Articles 14-27*

4. Training — Operational training and certification — *Article 28*

5. Compliance — Responsibilities, Testing, Analysis (incl. PI) — *Articles 29-31*

6. Final provisions — *Articles 32-33*

Annex I Incidents Classification Scale

Article 12 Protection *(cont'd)*

Objective

- the objective of protection is to ensure system security with well functioning, selective, reliable and redundant protection system
- the TSOs to cooperate with each other, DOSs and with Significant Grid Users to maintain coordination of protection principles and used set-points
- the security, reliability and redundancy of System Protection Schemes (SyPS) shall be on the same level, which is dominant elsewhere in power systems

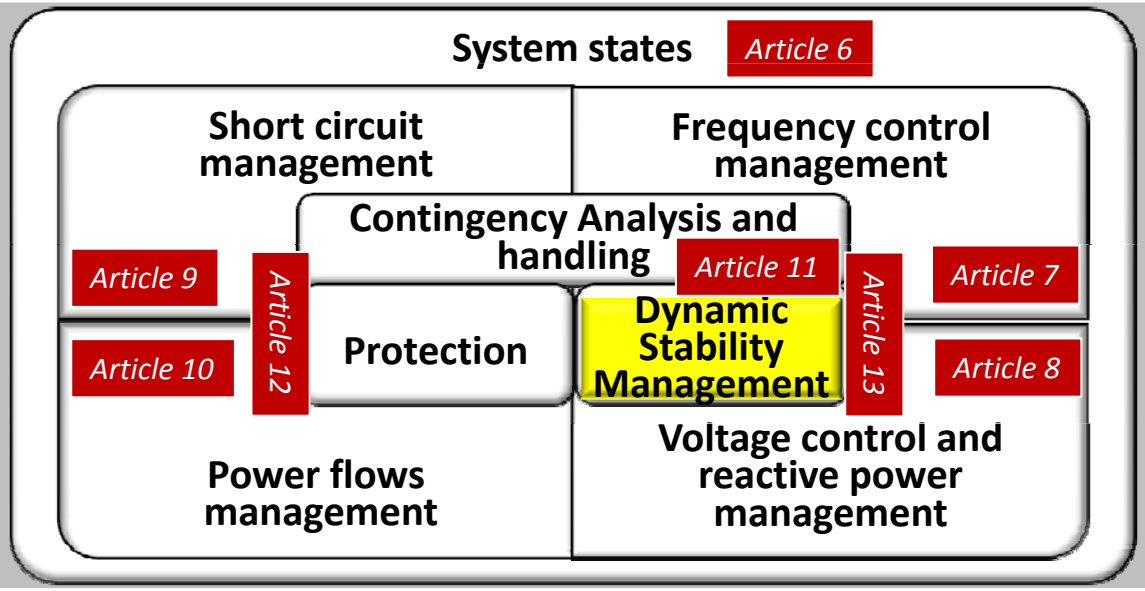
Article 12 Protection *(cont'd)*

- 27 comments were received on this Article
- the following were introduced
  - Deletion of word "endeavour" in order to clearly define the TSOs responsibility of reliable protection system
  - Fault Clearing Time for transmission system faults having stability impact was added in a new requirement
  - Coordination of protection between parties was added e.g. over-frequency protection and synchronism check (vector angle shift) during reconnection
  - DSOs in addition to Significant Grid Users have been added, where DSOs are affected or responsible parties in coordination of protection functions

Article 13 Dynamic stability management

1. General provisions: Subject matter and scope, Definitions, Regulatory aspects, Recovery of costs, Confidentiality obligations — *Articles 1-5*

2. Requirements



3. Data exchange — Data exchange — *Articles 14-27*

4. Training — Operational training and certification — *Article 28*

5. Compliance — Responsibilities, Testing, Analysis (incl. PI) — *Articles 29-31*

6. Final provisions — *Articles 32-33*

Annex I Incidents Classification Scale

Article 13 Dynamic stability management *(cont'd)*

Objective

- the objective of Dynamic Stability Management is to indentify system Stability Limits and take necessary measures if any stability violations occur
- when the stability limits are prevailing the DSA calculation shall be based on near realtime calculation

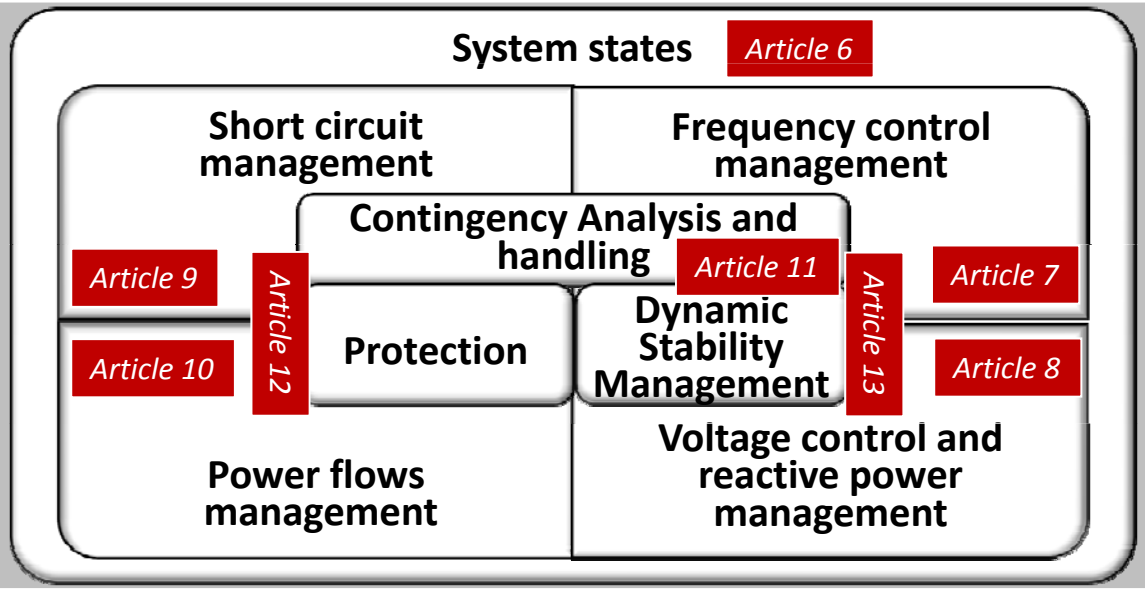
Article 13 Dynamic stability management *(cont'd)*

- 7 comments were received on this Article
- The following amendments were introduced
  - stability limits i.e. voltage, rotor angel and frequency, were added to be more precise in definition
  - in case of a violation of stability limits, TSOs shall implement measures to keep system stability, if necessary together with DSOs and Significant Grid Users
  - the methodology of the amount of needed inertia shall be established in cooperation between TSOs having reference to Article 3(3) and procured in a market based way
  - appropriate real time measurements shall be used and exchanged between the affected parties in order to be able to visualize dynamic stability parameters

Chapter 3 Data exchange

1. General provisions: Subject matter and scope, Definitions, Regulatory aspects, Recovery of costs, Confidentiality obligations — *Articles 1-5*

2. Requirements



3. Data exchange — Data exchange — *Articles 14-27*

4. Training — Operational training and certification — *Article 28*

5. Compliance — Responsibilities, Testing, Analysis (incl. PI) — *Articles 29-31*

6. Final provisions — *Articles 32-33*

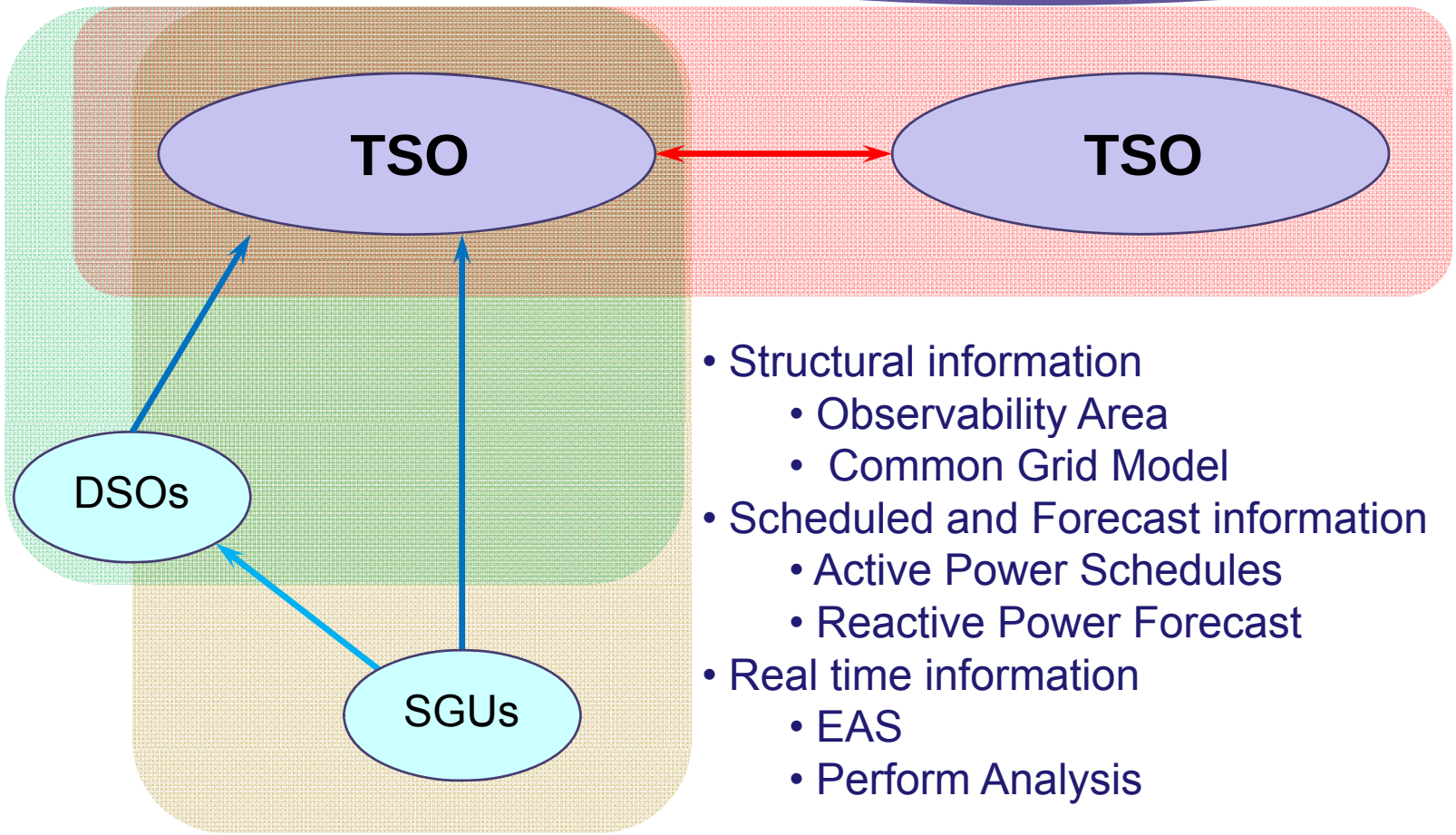
Annex I Incidents Classification Scale

Chapter 3 Data exchange *(cont'd)*

Objectives

- Describe the information needed by the TSO.
- Give the TSO the means to receive all necessary information to guarantee operational security by:
  - building and accurate model of the responsibility and obserbavility area.
  - Have real time information to efficiently define the System state
- Establish the necessary flow of information from DSOs, generator and grid users to the TSOs and between TSOs.

Chapter 3 Data exchange *(cont'd)*



- Structural information
  - Observability Area
  - Common Grid Model
- Scheduled and Forecast information
  - Active Power Schedules
  - Reactive Power Forecast
- Real time information
  - EAS
  - Perform Analysis

Chapter 3 Data exchange *(cont'd)*

Public Consultation

260 comments were received on Chapter 4 "Data Exchange". These were the main issues raised:

- Definition of Significant Grid Users
- NRA involvement
- Information for Distributors and Significant Grid Users
- Definition of Relevant DSO
- Detailed content of Data
- Coherence with other Network Codes

Some other comments were made to clarify the understanding of the code.

Chapter 3 Data exchange *(cont'd)*

Main amendments introduced in the Code:

- Significant Grid Users have been defined in Article 1(3) to precisely establish the systems Users affected by the code.
  New paragraph 14(4) has been included to adjust the threshold of Significance only for Data Exchange provisions.

- New paragraph 14(6) has been included to provide information to the Significant Grid Users and DSOs about the Transmission System at their Connection Point.

Chapter 3 Data exchange *(cont'd)*

- NRA involvement has been included in Article referred to threshold of Significance, detailed content of the Data, definition of Observability Area in the Distribution Network, communication between TSO and SGU connected to the Distribution Network and Aggregation of data for "small" SGU.

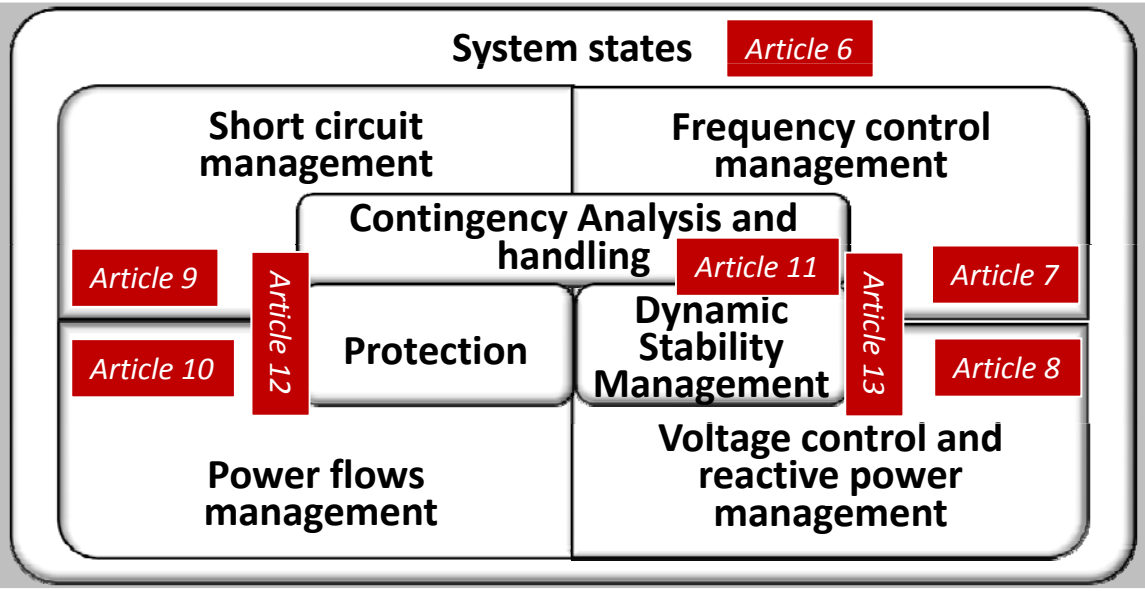
- "Relevant DSO" definition has not been included as it is not needed. The DSOs affected by this Network Code are those directly connected to the Transmission System or those that have Significant Grid Users connected to their Networks.

Other minor changes were made to adopt comments and improve the clarity of the Code.

Chapter 4 Training

1. General provisions: Subject matter and scope, Definitions, Regulatory aspects, Recovery of costs, Confidentiality obligations — *Articles 1-5*

2. Requirements



3. Data exchange — Data exchange — *Articles 14-27*

4. Training — Operational training and certification — *Article 28*

5. Compliance — Responsibilities, Testing, Analysis (incl. PI) — *Articles 29-31*

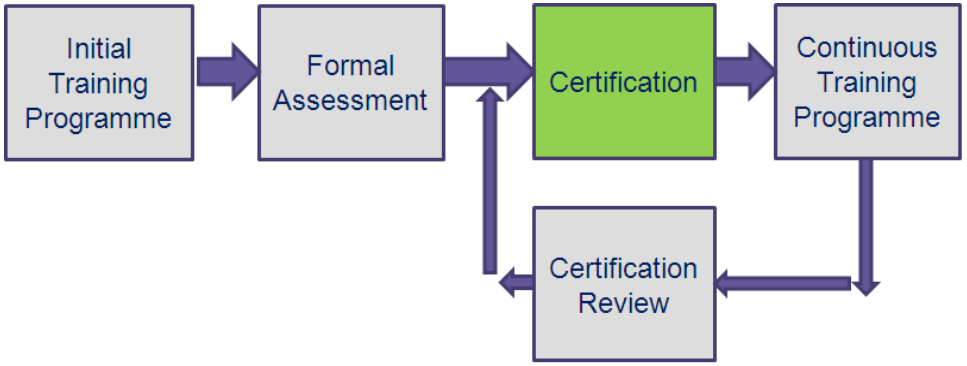
6. Final provisions — *Articles 32-33*

Annex I Incidents Classification Scale

Chapter 4 Training *(cont'd)*

Training &Certification ensures **education, on the job training and certification of TSOs' staff** responsible for System Operation in general and Operational Security in particular and provides for **coordinated and coherent training and certification approach of all European TSOs**.

- Documented training schemes for the TSO control room System Operators.
- Training programmes: dealing with normal and emergency conditions, includes inter TSO influences; reflect new technologies and changing conditions.
- Formal certification process.
- Coordinated training between TSOs and with input from System Users.



Chapter 4 Training *(cont'd)*

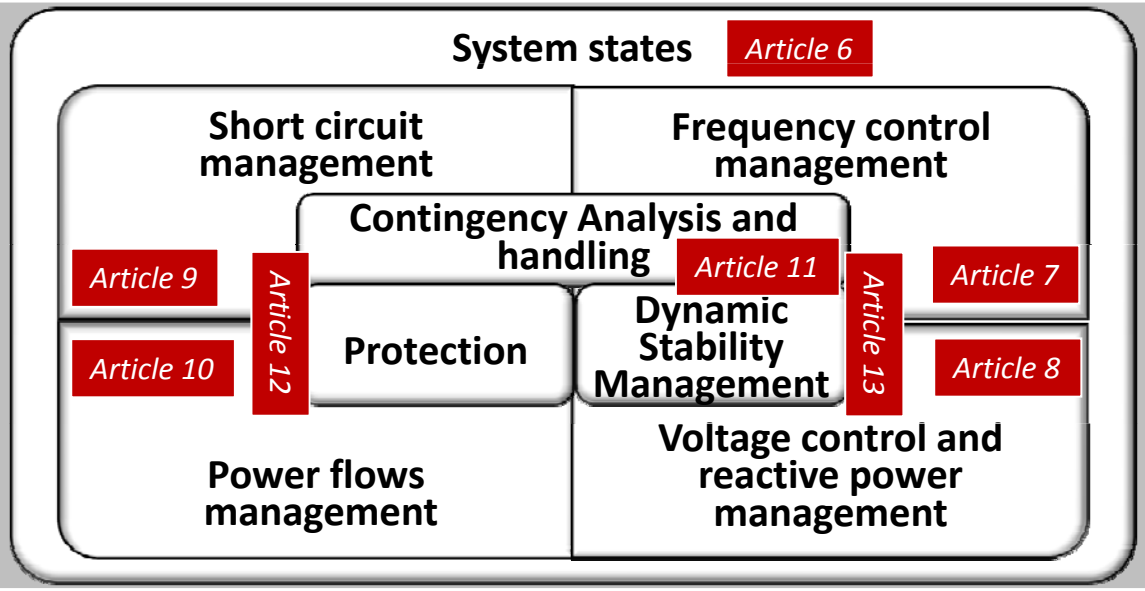
- 18 comments were received on Training and Certification
- No significant issues raised, mainly clarification suggestions, comments were broadly in three themes
  - Explicitly state training covers all states (including black-out and restoration)
  - Shared training with DSO, Significant Users (eg Nuclear stations)
  - NRA involvement

- Virtually all comments fully adopted as they aided clarity
- NRA involvement comments partially adopted
  - Now explicitly states a TSOs scope and details of its training processes are shared with its NRA
  - NRA approval of competencies for an Operator and for the NRA approval of an extension of an Operators Certification were not adopted

Chapter 5 Compliance

1. General provisions: Subject matter and scope, Definitions, Regulatory aspects, Recovery of costs, Confidentiality obligations — *Articles 1-5*

2. Requirements



3. Data exchange — Data exchange — *Articles 14-27*

4. Training — Operational training and certification — *Article 28*

5. Compliance — Responsibilities, Testing, Analysis (incl. PI) — *Articles 29-31*

6. Final provisions — *Articles 32-33*

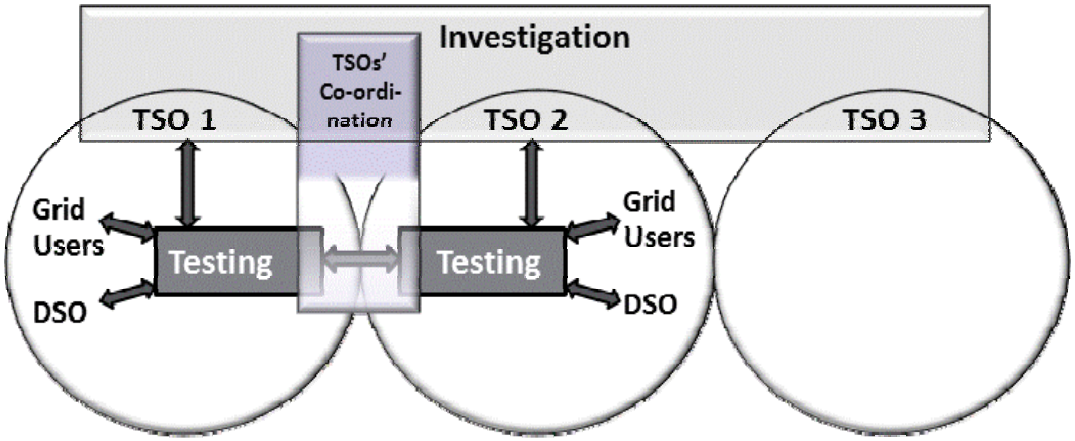
Annex I Incidents Classification Scale

Article 30 Responsibilities of TSOs & DSOs

- **Art. 30: Operational Security Performance Indicators**
  - Art. 30(1)(a): means within the own Responsibility Area of TSOs
  - Art. 30(1)(b): means through cooperation with other stakeholders
  - Art. 30(1)(c), (d): enhancements based on annual reporting / ICS
  - Art. 30(2): annual reporting based on Operational Security Performance Indicators from ICS
  - Art. 30(3): Operational Security Ranking

Article 31 (former 14) Common testing and incidents analysis

The aim of Common testing and incident analysis is to ensure correct functioning of transmission system elements, processes and significant grid user facilities and that testing is planned and coordinated.



- *Ensure correct functioning of system elements.*
- *Allow TSOs, DSOs and Significant Grid Users to test their plant.*
- *Continuing compliance of Significant Grid Users with requirements of this code and with declared ancillary services.*
- *Planning and coordination of operational tests.*
- *Analysis of power system incidents.*

Article 31 Common testing and incidents analysis *(cont'd)*

93 comments were received on Testing and Investigation

On the overall former Article 14

2 comments were received and 4 requests for additional Articles. The main theme was:

1) Move to Compliance chapter

Rationale for Change/ No change

Moved to Compliance chapter

Agree with DSOs and Stakeholders on cost recovery and information exchange from TSOs, NRA involvement and publication will ensure transparency. Proposed new articles on cost recovery, involvement of NRA in incident analysis and publication added, TSO and DSO to provide to information for Significant Grid User investigation.

former Article 14(1)

8 comments were received. The main themes were:

1) Practicality 2) Definition of Ancillary Services 3) Inability of ageing plant 4) Consistency with RfG 5) Continuous monitoring

Rationale for Change/ No change

Definition of Significant Grid User allows the exemption of "small" grid users. Definition of Ancillary Service has been added. A Grid User will not be required to do anything that it has not declared itself capability of. Continuous monitoring removed as it may not be appropriate in all situations.

Article 31 Common testing and incidents analysis *(cont'd)*

former Article 14(2)

11 comments were received. The main themes that emerged:
1) Involvement of DSO 2) Contract provisions prevail 3) Significant Grid Users are deemed compliant after initial compliance testing 4) Recording notification 5) TSO obligation 6) Practicality 7) Monitoring operational security

Rationale for Change/ No change

This requirement has been modified to include DSO involvement and includes that contract provisions prevail. For the TSO to meet its obligation to ensure operational security of the transmission system, it should have the ability to check that the services offered by Significant Grid Users to achieve this goal are available when required. Recording has been removed. Definition of Significant Grid User allows the exemption of "small" grid users. Monitoring of operational security is covered by other articles of this code.

former Article 14(3)

2 comments were received. The main theme was:
1) Not in TSO's remit or scope

Rationale for Change/ No change

For the TSO to meet its obligation to ensure operational security of the transmission system, it should have the ability to monitor that the provision of services by Significant Grid Users which they are required or have agreed to provide.

Article 31 Common testing and incidents analysis *(cont'd)*

former Article 14(4)

2 comments were received. The main themes were:
1) Limited to reasonable required relevant information 2) Practicality

Rationale for Change/ No change
Agree with DSOs and Stakeholders on reasonable and relevant information. Definition of Significant Grid User allows the exemption of "small" grid users.

former Article 14(5)

4 comments were received. The main themes were:
1) Is ICS legally binding (changes through comitology) 2) Specify level 2

Rationale for Change/ No change
The two requirements related to the incidents classification scale have been combined into one and the incidents classification scale document will form an annex to this code.

former Article 14(6)

11 comments were received.
The main themes were: 1) This is covered by the RfG NC and the DCC 2) Practicality

Rationale for Change/ No change
Agree with DSOs and Stakeholders to remove the Article

Article 31 Common testing and incidents analysis *(cont'd)*

former Article 14(7)

5 comments were received. The main themes were:
1) should be in RfG 2) Practicality

Rationale for Change/ No change
Agree with DSOs and Stakeholders up to a point. There should be a test plan developed. It is covered by two other requirements, provision of information to the TSO and the TSO analysis and planning. Definition of Significant Grid User allows the exemption of "small" grid users.

former Article 14(9)

4 comments were received. The main theme was:
1) Impact on Significant Grid Users

Rationale for Change/ No change
Agree with DSOs and Stakeholders the impact on Significant Grid Users has been included.

former Article 14(10)

5 comments were received. The main themes were:
1) Cost recovery 2) DSO and Significant Grid User Security

Rationale for Change/ No change
Agree with DSOs and Stakeholders on the inclusion of safety and have added a new requirement on cost recovery.

Article 31 Common testing and incidents analysis *(cont'd)*

former Article 14(11)

14 comments were received. The main themes were:
1) Costs 2) Agreed by all 3) Non-discrimination and transparency 4) Imprecise

Rationale for Change/ No change
Agree with DSOs and Stakeholders to remove the Article

former Article 14(12)

3 comments were received. The main themes were:
1) Cost recovery 2) Significant Grid User safety

Rationale for Change/ No change
A requirement on cost recovery has been added and the ability of a DSO or Significant Grid User to postpone or interrupt a test has been added.

former Article 14(13)

3 comments were received on this Article 31(13). The main themes were:
1) specify TSO responsibility and time frame 2) Practicality 3) Public availability of system state

Rationale for Change/ No change
The requirement as it was in Chapter 14 has been deleted as it was duplicated in the Compliance chapter. It is difficult to put an exact time frame on the provision of test information. More complex test will require more time to plan for where as less complex test may require very little time. If required we can specify a time frame that covers all tests. Definition of Significant Grid User allows the exemption of "small" grid users. Publication of the system state may only be of benefit for short notice within day tests.

Article 31 Common testing and incidents analysis *(cont'd)*

former Article 14(15)

2 comments were received. The main theme was:
1) Publication of analysis

Rationale for Change/ No change
Agree with DSOs and Stakeholders, publication of analysis is included.

former Article 14(16)

2 comments were received. The main themes were:
1) Consistency with RfG 2) Practicality

Rationale for Change/ No change
Due to duplication with a more general article in the Compliance chapter this article was removed. The more specific information requirements are probably too detailed for a pan-European network code and are probably best covered at national level.

former Article 14(17)

5 comments were received. The main themes were:
1) risk and remedial actions 2) level of detail 3) Information to DSOs

Rationale for Change/ No change
Agree with DSOs and Stakeholders, information to be provided to the affected DSOs, risk mitigation and remedial actions included and all the details of the test to be provided.

Article 31 Common testing and incidents analysis *(cont'd)*

former Article 14(18)

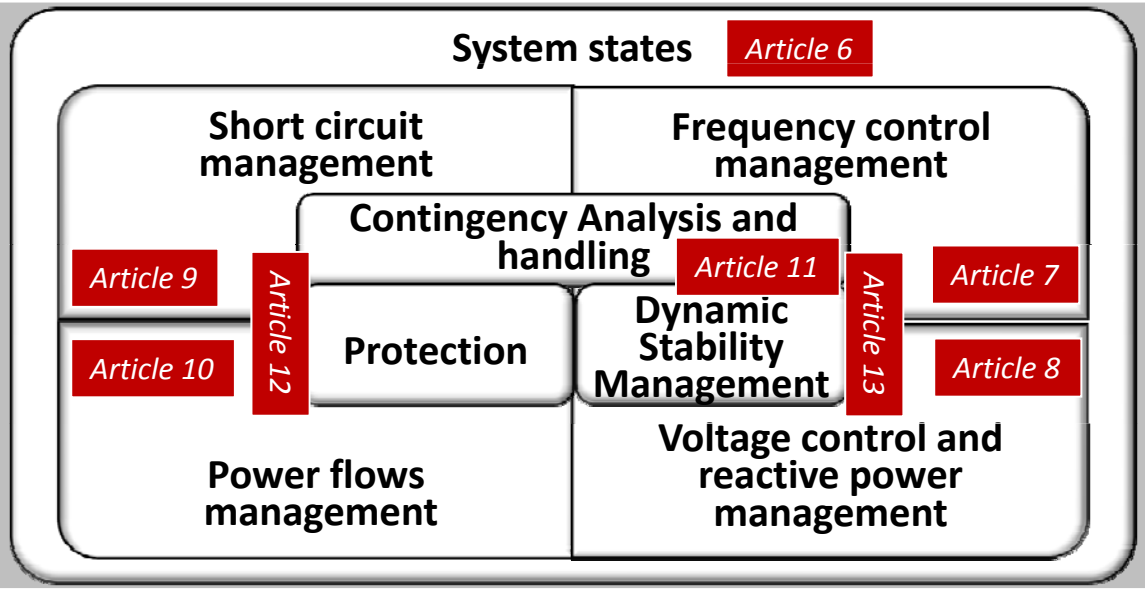
2 comments were received. The main themes were:
1) Group analysis 2) Relevant and reasonable information

Rationale for Change/ No change
Requirement changed to be more equitable to all parties. For group analysis was unsure of confidentiality implications of one Significant Grid User analysing the response of another. Relevant and reasonable information added.

Chapter 6 Final provisions, Annex I ICS

1. General provisions: Subject matter and scope, Definitions, Regulatory aspects, Recovery of costs, Confidentiality obligations — *Articles 1-5*

2. Requirements



3. Data exchange — Data exchange — *Articles 14-27*

4. Training — Operational training and certification — *Article 28*

5. Compliance — Responsibilities, Testing, Analysis (incl. PI) — *Articles 29-31*

6. Final provisions — *Articles 32-33*

Annex I Incidents Classification Scale

Chapter 6 Final provisions, Annex I ICS

- **Art. 33: entering into force in 2 (former 3) years**

- **Annex I: ICS …**

Thank you for your attention

OS NC 4th Workshop | Tahir Kapetanovic |
20.12.2012

entsoe

Reliable Sustainable Connected