



Network Code on Operational Security

User's Group System Operations
06/11/2013



Agenda

- **Objectives of Network Codes**
- **Operations codes vs. Connection codes**
- **System Operation NC and NC OS**
- **State of play of NC OS**
- **Contents: ACER's opinion of 28/05/2013 and code adjustments**

Agenda

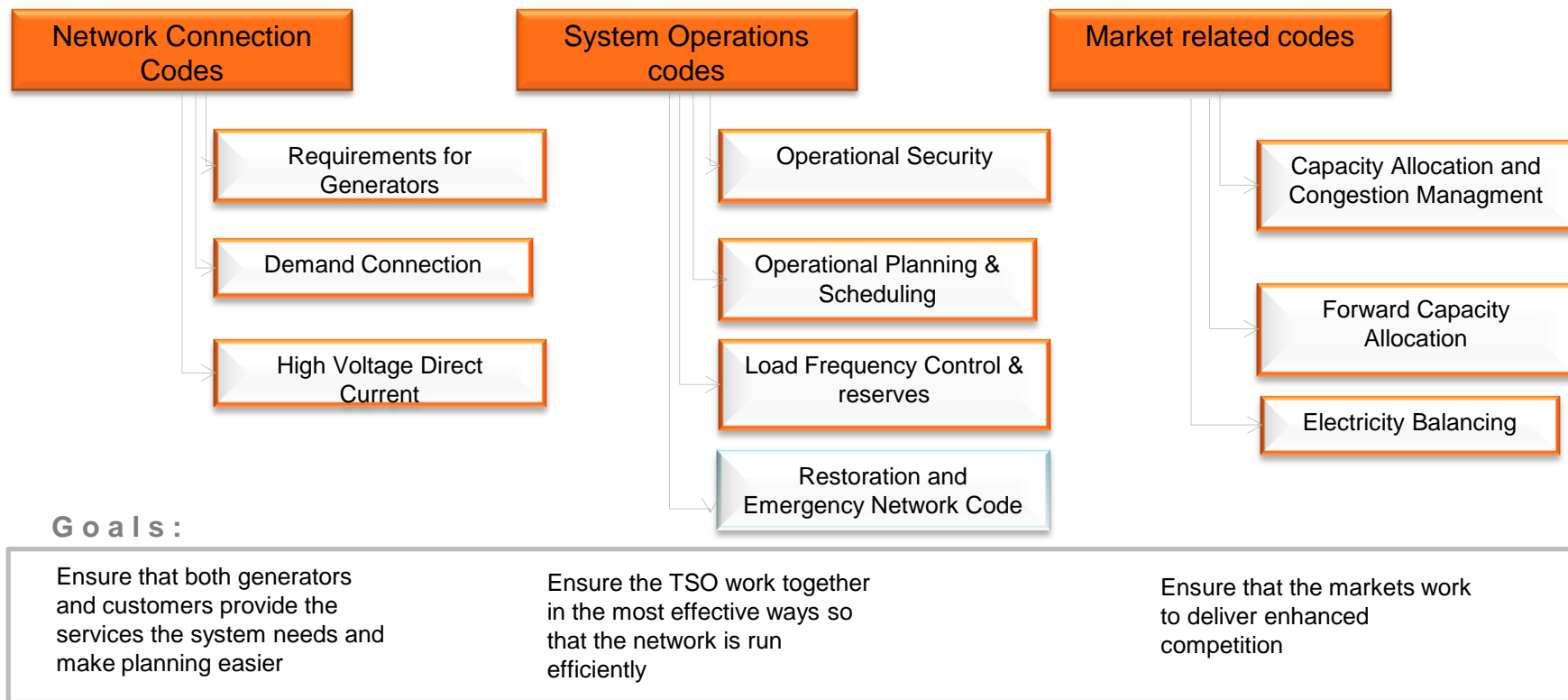
- Objectives of Network Codes
- Operations codes vs. Connection codes
- System Operation NC and NC OS
- State of play of NC OS
- Contents: ACER's opinion of 28/05/2013 and code adjustments

The objectives of the network codes



For : delivering **secure, competitive and low carbon** European electricity market by :

- Developing and reinforcing **transmission networks**
- Operating systems in a more **coordinated** manner
- Facilitating the development of a **pan-European electricity market**
- Ensuring all **system users** are able to contribute to the stable and secure operation of the transmission system.



Connection and Operation codes

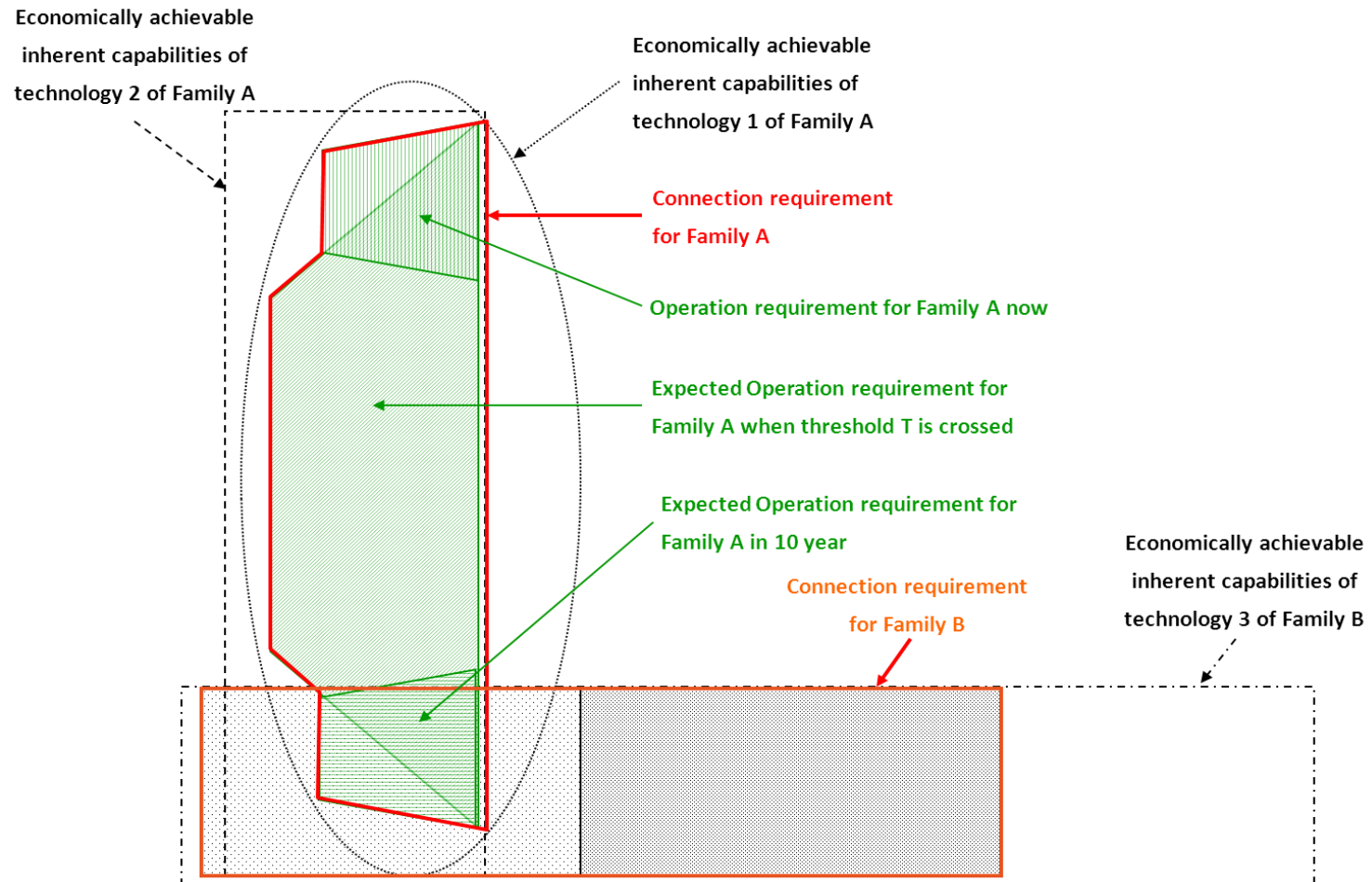


- Operation principles and criteria
 - Reviewed periodically by TSOs to operate the grid in the most efficient way, taking into account the evolution of the system (generation and load firstly)
 - Applies to network operators mainly, and to significant users participating to grid support services
 - Constrained by grid user's technical capabilities
- Connection of grid users
 - Technical capabilities defined at the investment phase and difficult to change
 - Grid user's equipment lasts several decades
 - Need to be prospective and include everything that we can *reasonably* expect to be needed in the future
- As a consequence, **operation codes will not provide a complete justification of the requirements set for grid users in the connection codes**

Connection and Operation codes



Illustration: J. Sprooten, J. Warichet, T. Haase, “Connection and Operation Requirements for the Integration of Offshore Generation in Power Systems”, *RevueEtijschrift* (to be publ.)



Agenda

- Objectives of Network Codes
- Operations codes vs. Connection codes
- **System Operation NC and NC OS**
- **State of play of NC OS**
- **Contents: ACER's opinion of 28/05/2013 and code adjustments**

Operational Security

Objective

- Maintain Operational Security **24 hours a day, 365 days a year** by providing the global Operational Security **Framework**.
- Focus on **common operational security principles**, pan-European operational security, coordination of system operation, and some important aspects for grid users connected to the transmission grid.
- This code is the “**umbrella**” for the System Operation Codes (Operational Planning & Scheduling, Load Frequency & Reserves, Emergency code)
- This network code relies on the connection requirements of the DCC and RfG.

Applicability

- The code determines the roles and responsibilities for **TSOs, DSOs, significant grid users** and **market players**
 - the **significant users** are the one defined in the DCC and in the RfG :
 - redispatching **Aggregators** and **Providers of Active Power Reserve** according to the Network Code Load Frequency Control & Reserves are also significant users towards OS.
- “The network code(s) for System Operation shall elaborate on relevant subjects that should be coordinated between TSOs, as well as between TSOs and **Distribution System Operators (DSOs)**; and with significant grid users, where applicable”.

DCC : Demand Connection Code

RfG : Requirements for Generators

Operational Security

Long history

The Operational Security is built upon a long history of existing common best practices and lessons learned and operational needs

Challenges of today : be prepared for the future

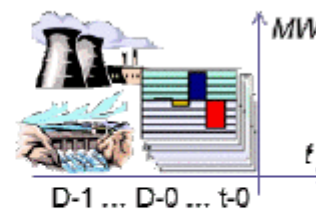
Key challenges



Intermittent generation
(wind, solar power)
with low predictability



Massive growth of
cross-border trade
and transits



Generation allocation
close to real-time and
continuously changing

Figure 29: Key challenges in the framework of System Operation (Source: ENTSO-E)

Cost Recovery

Costs assessed as efficient, reasonable and proportionate shall be recovered as determined by National Regulatory Authorities.

Operational Security

An “umbrella” network code

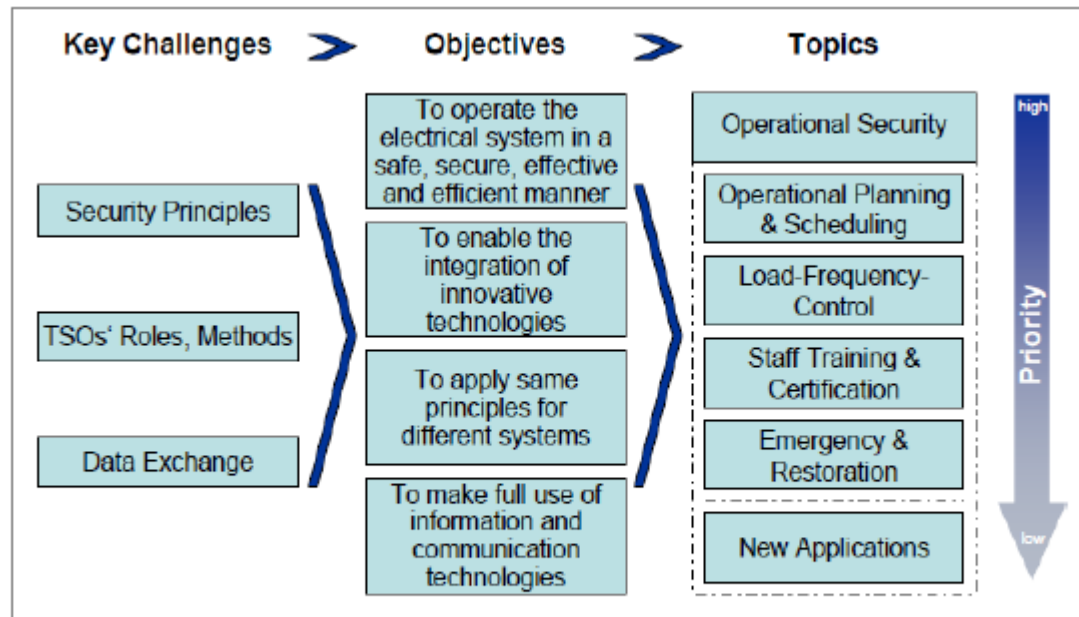


Figure 5: Structure and development flow of the Framework Guidelines on Electricity System Operation
(Source: [1])

	Network Code - Content	Status
<p>S N y e s t t w e o m r k O p C e o r d a e t s i o n</p>	<p><u>Operational Security (OS)</u></p> <p>Provides the global Operational Security Framework.</p> <p>Goal : maintain Operational Security 24 hours a day, 365 days a year.</p> <ul style="list-style-type: none"> • Sets out the common principles to be followed by all TSO • Align and harmonise operational security principles throughout Europe and make cooperation between network operators (TSO- TSO and TSO-DSO) and network users for the first time legally binding. 	<ul style="list-style-type: none"> • ACER has adopted its opinion (no recommendation) on 28 May 2013 • The final network code was resubmitted to ACER on 24 September 2013 • ACER will now have to publish its recommendation towards the EC (anticipated to November 2013) • Comitology could be expected Q1-Q2 2014 • Entering into force possibly end 2014 / 2015

Vision of Elia: What will change?



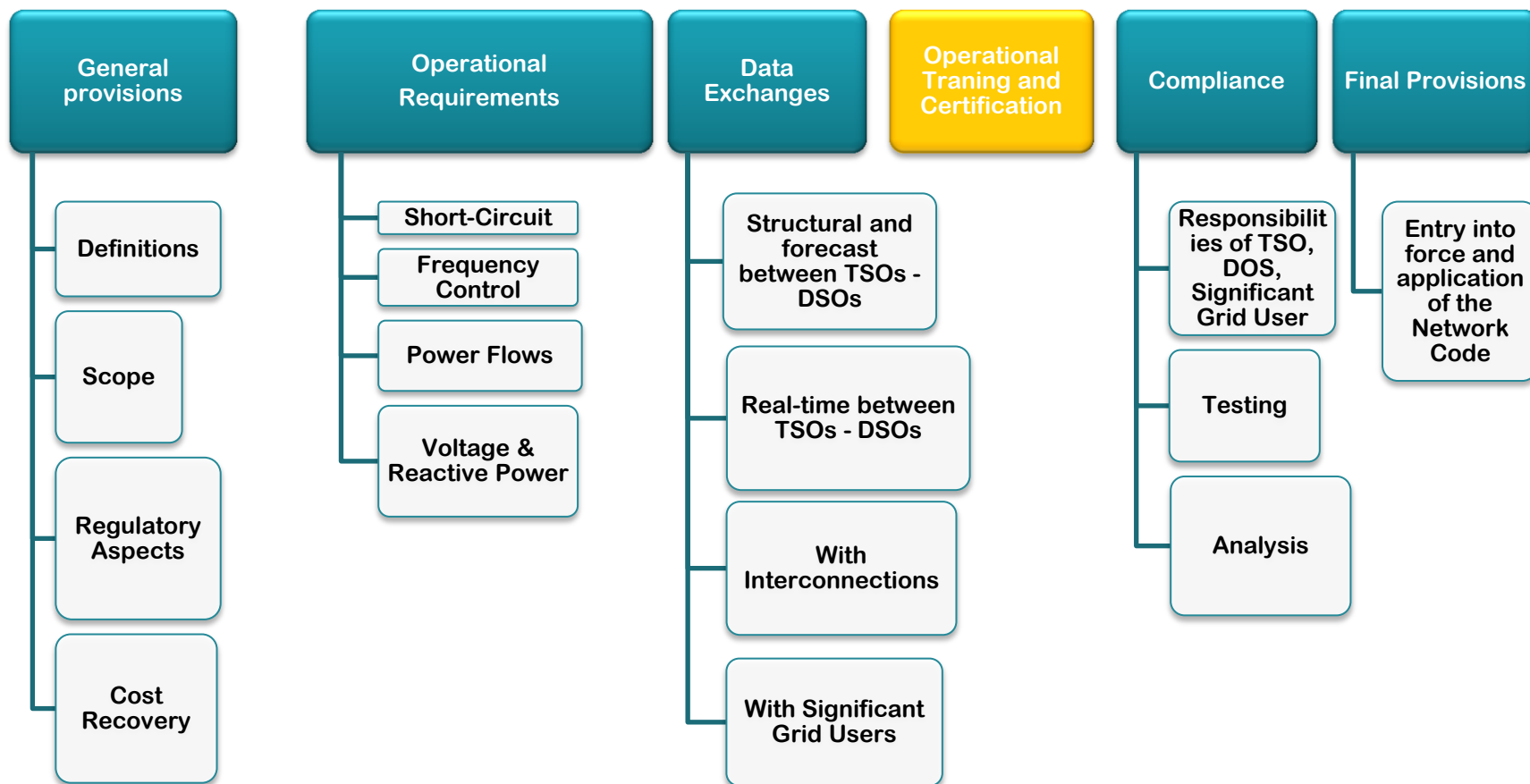
- Codes provide a legal framework
 - ENTSO-e experts have tried to identify all the **future issues of the system** that require being handled at the pan-European level
 - The codes allow decreasing regulatory or legal barriers to the implementation of solutions that might be necessary in the future, while leaving a sufficient freedom to member states / NRAs to define the details
- As a consequence, Elia will not change the current processes (if not for the better)
 - stakeholders should not fear that Elia will have the power to unilaterally impose new requirements without reflection and consultation
 - Platforms of consultation: Synergrid, User's group, etc.
 - Regulators and Administration keep their responsibility of approving changes
 - Where needed and feasible, CBA will be performed


Agenda

- Objectives of Network Codes
- Operations codes vs. Connection codes
- System Operation NC and NC OS
- State of play of NC OS
- **Contents: ACER's opinion of 28/05/2013 and code adjustments**

Operational Security

Chapter structure



 The operational training and certification part of the code will probably become a regulation apart from the Network Codes.



- I. Coherence & compatibility with other network codes
 - II. National scrutiny → *NRA involvement*
 - III. Performance indicators → *„per country“*
 - IV. Information exchange → *DSO & SGU proportionality*
 - V. Scope → *non-interconnected systems*
 - VI. Drafting quality
- ... all in all ...

NC OS broadly in line with FG; PI only subject-matter issue

The key priorities for adjustments of the Code



*The „final product“ to meet
the EC expectations for
comitology*

*The adjustments to give
ACER basis for a final
recommending opinion*

*Consider additional DSOs'
concerns wherever possible*

**NO compromising on
Operational Security**

Summary of what / where has been adjusted in the Code

Specific coherence with OPS
& LFCR, no „best endeavour“,
SGU & DSO issues

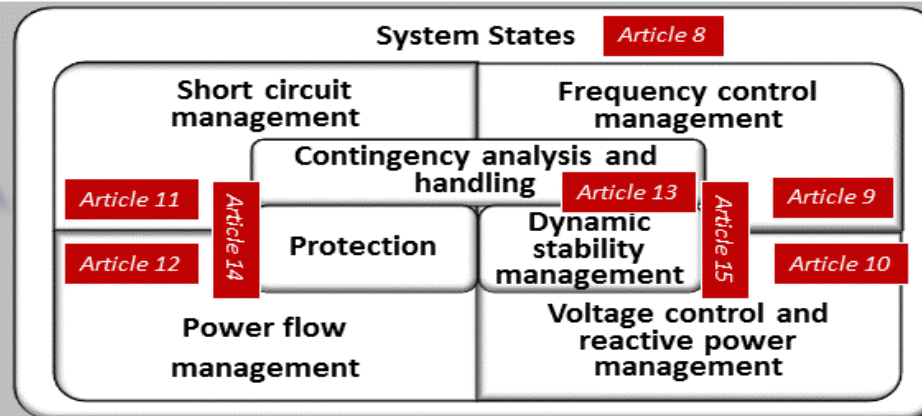
General coherence all
NC: national scrutiny,
scope & Definitions

1. GENERAL PROVISIONS: Subject matter and scope, Definitions, Regulatory aspects and approvals, Recovery of costs, Confidentiality obligations, Agreements with TSOs not bound by this Network Code

Articles 1-7

DSOs' & SGUs
proportionality, clarity

2. OPERATIONAL SECURITY REQUIREMENTS



3. DATA EXCHANGE

Articles 16-29

4. TRAINING

Operational training and certification

Article 30

5. COMPLIANCE

Articles 31-33

Responsibility of the SGUs

TSOs, DSOs Responsibilities

Common testing & analysis

Amendments

Entry into force

6. FINAL PROVISIONS

Article 34-35

I. Coherence & compatibility of network codes



- **Recitals (↓, not legally binding)**
 - Removed explanatory ones, Recitals 4-6 agreed with DSOs, Added Recital 10 on MS powers and NRA involvement, added 24 on CACM
- **Article 1(3) & 1(4) on multiple TSOs added, for all codes, Removed Article 1(5) on nuclear safety and updated 1(7) on good industry practice**
- **Article 2: removed definitions of Business Continuity Plan (explanation in Art. 8(16)), Time to Restore Frequency (→ NC LFCR) and refined def's of SGU, Synchronous Area and Virtual Tie-Line**

I. Coherence & compatibility of network codes *(cont'd)*

- Article 3 **Regulatory aspects**: removed part of Art. 3(3) and Art. 3(5) on nuclear safety to avoid redundancy
- Article 5 **Recovery of costs**: remove 5(4) compliance test costs
- Article 7 amended with 7(3) for cases when **Agreement pursuant to 7(1) and 7(2)** cannot be implemented
- Article 35. adjusted accordingly

II. National scrutiny

Article 4 **Regulatory approvals** → amended with

- Art. 4(2)(d) on **criteria for requesting compliance test**
- Art. 4(2)(e) on **high priority SGU** cf. Art. 32(10)
- Art. 4(2)(f) on **SGU data provision exemptions** cf. Art. 27(2)

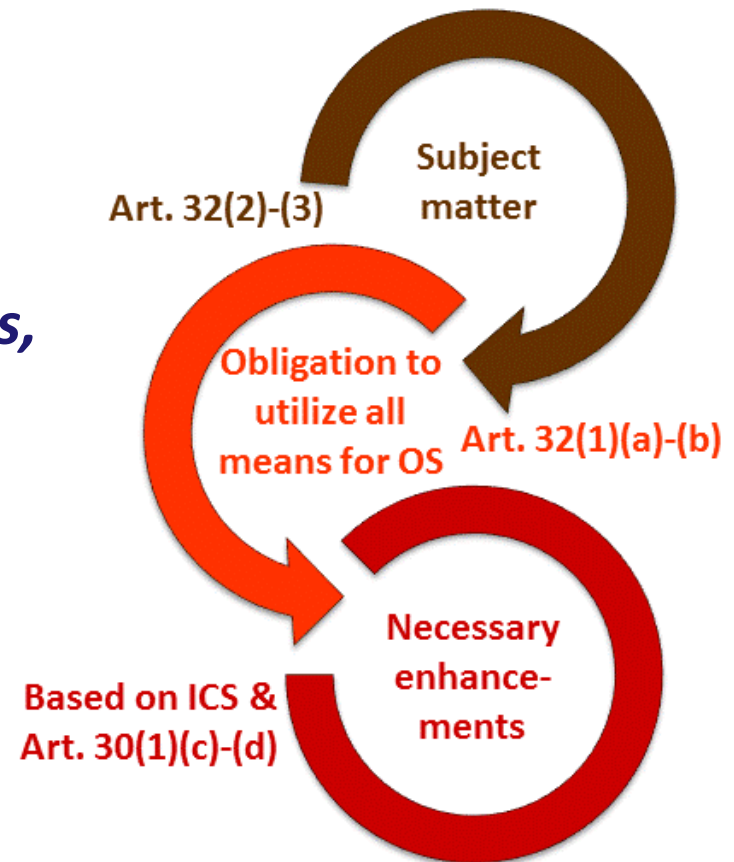


The key concepts & process:

Therefore, added in Art. 31(2)

- **geographical scope,**
- **electrical TSO interdependencies,**
- **historical information**

to be reflected upon, for incidents
in annual report.



IV. Information exchange

- Modification of Art. 16(6)-(8) in the sense of **DSOs' proposal**
- „**best available**“ for DSO aggregated data in Art. 20(1)
- Amendments in Art. 27(1)-(2) on **SGUs' obligation to deliver data also to DSOs**
- New Art. 31(9) for **Type A User not tested** but only their Aggregators must be compliant with the requirements

- Art. 1(4) added with „***no applicability to the TSO or part of a TSO which are not synchronously interconnected***“
- Also, no application to the Åland Islands

VI. Drafting quality



- Art. 8(14): precise on TSO „... *instructing the SGUs ...*“
- Art. 10(4), new, on **Demand Facilities capabilities/disconnect**
- Accepting DSOs proposals in Art. 10(13), 16(6) and 16(8) in the sense of **proportionality**
- Corrected **Art. 12(3) „Responsibility Area“ → „Observability Area“**
- Art. 13(10) added „convergence of load-flow calculations“ as the meaning of „sufficiently“

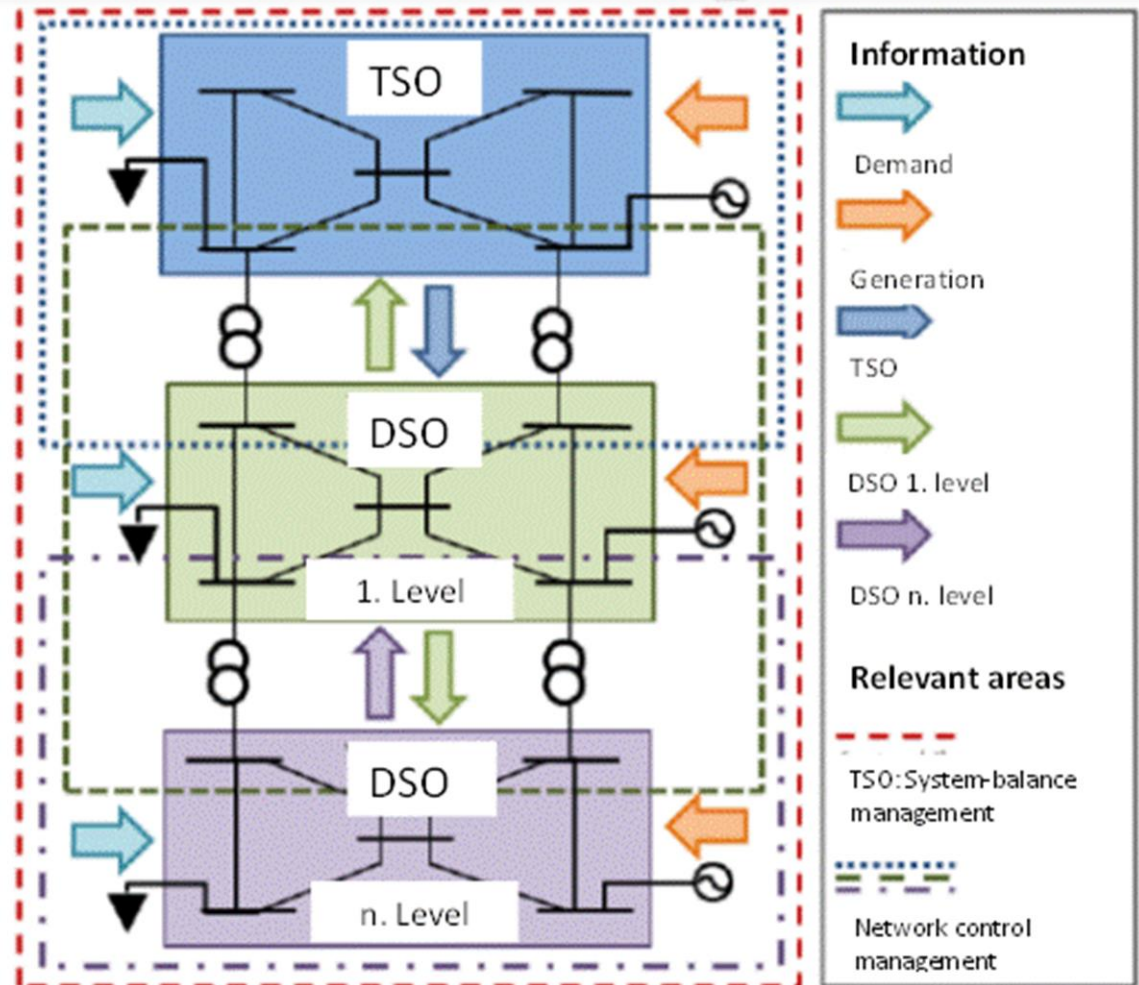


- *„Transmission Connected Demand Facilities“*
- *„Best endeavour“ → „use all available economically efficient and feasible means under its control“*
- *„European Awareness System“ → „IT tool for real-time data exchange“, to reduce need for new definitions*
- **Wording and rephrasing of several articles**



- Chapter 3.5: **compliance by each TSO**, if an agreement at the Synchronous Area cannot be achieved → greatest possible extent for Code implementation throughout Europe
- Chapter 6.5: **flexibility and proportionality in data exchange** for DSOs and SGUs & **flexibility cf. real-time data for A**
- Chapter 6.7.4: **Examples on operational data exchange** → ...

...➔ key principles
of data &
information
exchange
between grid
operators



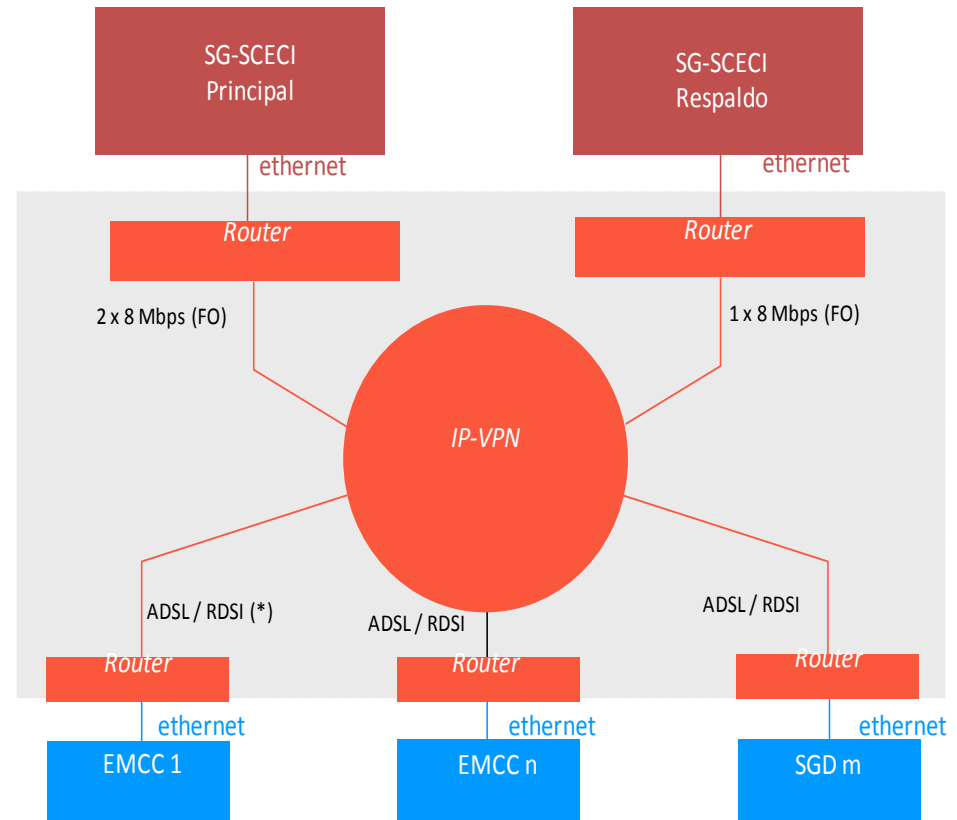
Adjustments in Supporting Document *(cont'd)*

...➔ **direct communication with SGUs providers of special services (e.g. here: interruptible loads)**

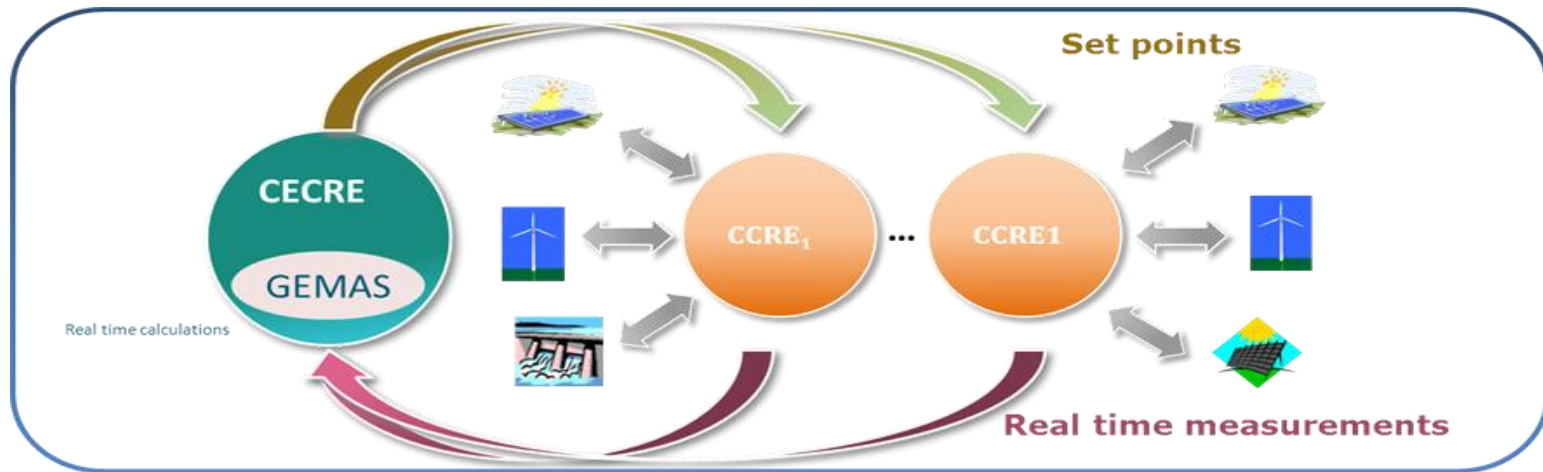
TSO System including monitoring

Communication channels directly with SGUs participating in the service

SGU System including activation of instructions



...➔ real-time communication to the control-centres of intermittent/renewable generation, depending on Operational Security needs





- Chapter 7.4.1: Clarifying explanation on **geographical, electrical and history** scope and characteristics for Performance Indicators
- Chapter 8.2.1: underlying clarification that the **SGU concepts address Aggregators** and not their individual small members
- Chapter 8.5.3: further detailed explanation on pre-fault and post-fault Remedial Actions
- Annex III adapted to fit new Article 4 of the Code

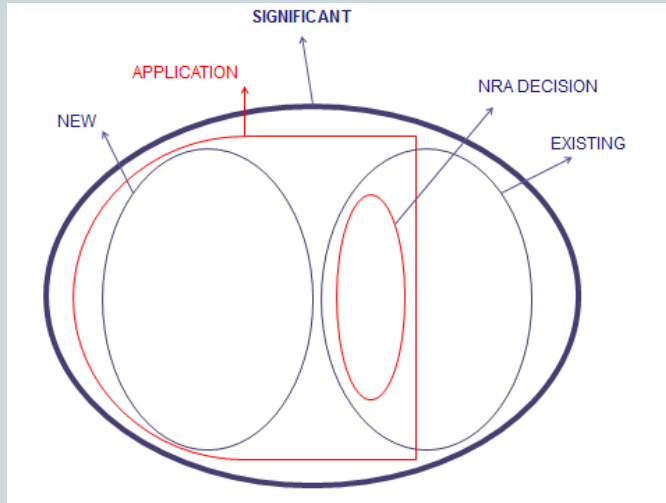


- Annex V (FAQ) amended with explanations of **real-time** and **Virtual Tie-Line**
- Annex VIII (Definitions) aligned with the Code

Backup slides

Approach to « significance »

“APPROACH 1”



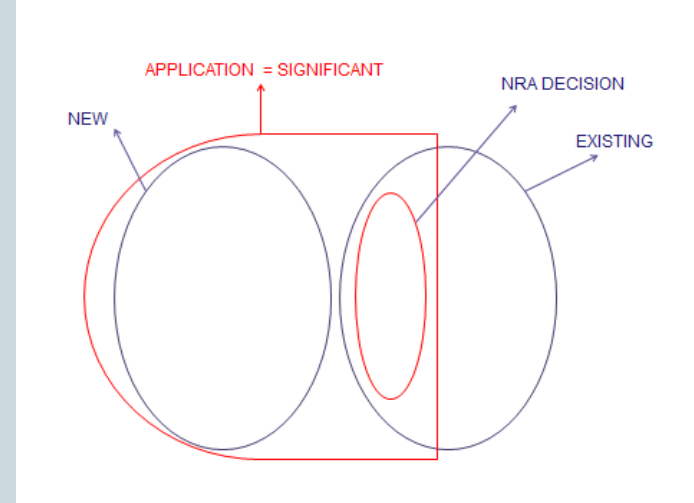
Variables for determining **significance**:

- Influence on control area's security of supply

Variables for determining **application**

- Influence on control area's security of supply
- New-Existing variable
- Procedure ending in NRA decision

“APPROACH 2”



Variables for determining **significance & application**:

- Influence on control area's security of supply
- New-Existing variable
- Procedure ending in NRA decision

System Operations Codes > Emergency and Restoration

Emergency and Restoration

! The writing of the Code not yet started !

Following information from the ACER guidelines on **Operational Security:**

- **Scope & objectives**
 - Organize remedial actions in case of emergency fastly, effectively, reliably an as efficiently as possible
 - Ensure restoration after major disturbance or blackout are well coordinated and led by the TSOs
- **Criteria for emergency and restoration shall include at least the following :**
 - Share of alert situations
 - Evidence of training, simulations, tests and exercises
 - Emergency prevention and restoration shall consider cost benefit issues on macroeconomic and market level.
- **Roles & Responsibilities**
 - TSOs are responsible for remedial actions and shall enforce orders to significant grid users
 - Restoration related organisation and procurement of black-start and islanding capabilities, as well as ancillary services shall be assigned by the TSO, which shall have the duty and power to decide on any subsequent applicability at the DSO level.
 - The DSO shall suport the restoration according to the plan
- **Information exchange**