Operational Security Code

3rd Workshop

18-19. September 2012

entsoe

Reliable Sustainable Connected

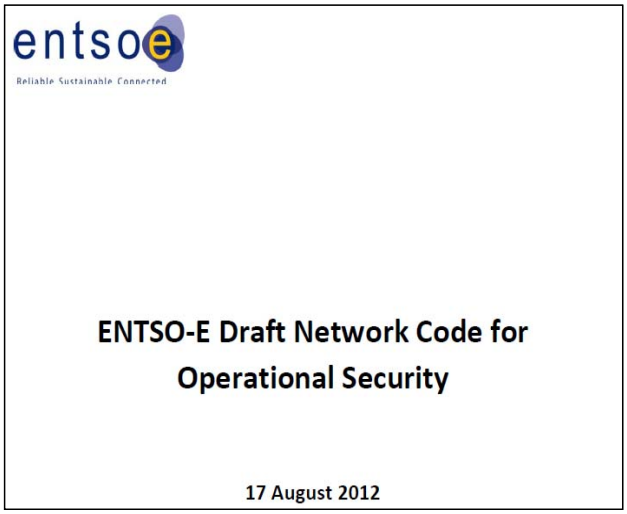
Highlights

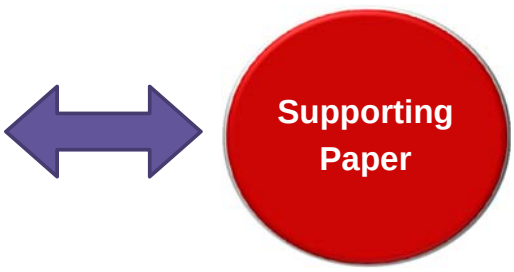
- Contents & structure (update)
- Key provisions (overview)
- Stakeholders‘ suggestions so far
- Next steps

Highlights

- Contents & structure (update)
- Key provisions (overview)
- Stakeholders' suggestions so far
- Next steps

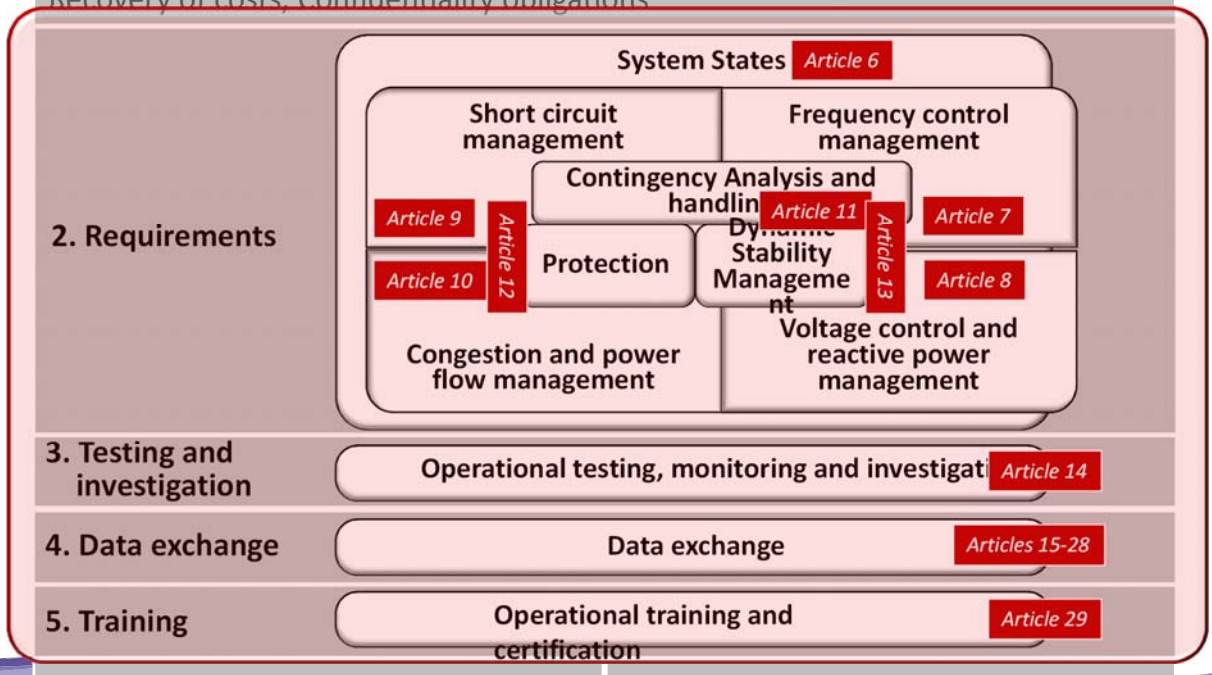
Structure





Contents

1. General Provisions: Subject matter and scope, Definitions, Regulatory as Articles 1-5
Recovery of costs, Confidentiality obligations



6. Compliance Articles 30-31

7. Final Provisions Article 32-33

Supporting Paper

1. Purpose and Objectives
2. Procedural Aspects
3. Scope, Structure & Approach to Drafting the OS NC
4. Relationship between the OS NC & FG
5. Objectives of the OS NC
6. Added Values of the OS NC
7. Responses and Next Steps (for PC …)
8. Literature & Links

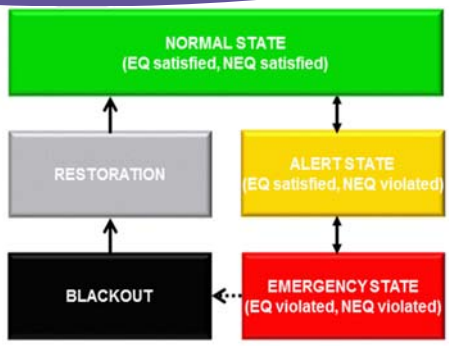
Highlights

- Contents & structure (update)
- Key provisions (overview)
- Stakeholders' suggestions so far
- Next steps

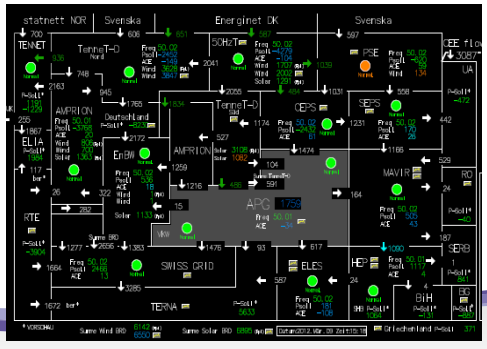
Chapter 2. Requirements (1/6)

Article 6: System States

- 5 system states
- Monitoring
- Estimation
- Operational Security Limits
- Preventive and remedial actions
- Operational Security Analysis
- Information / awareness system



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



Chapter 2. Requirements (2/6)

Article 7: Frequency Control Management

- Frequency quality, monitoring, measures
- New terms (FCR, FRR, …)
- Reserves / exchange
- Detailed implementation in the LFC&R NC (OS NC = „umbrella“ …)

Article 8: Voltage Control & Reactive Power Management

- Q-reserves
- Grid Users‘ obligations, automatic / manual measures
- Priorities: prevention of voltage collapse / system integrity

Chapter 2. Requirements (3/6)

Article 9: Short-Circuit Current Management

- Short-circuit currents: circuit breaker capacity vs. protection activation current
- Short circuit calculation: own grid and in cooperation with TSOs (and DSOs)

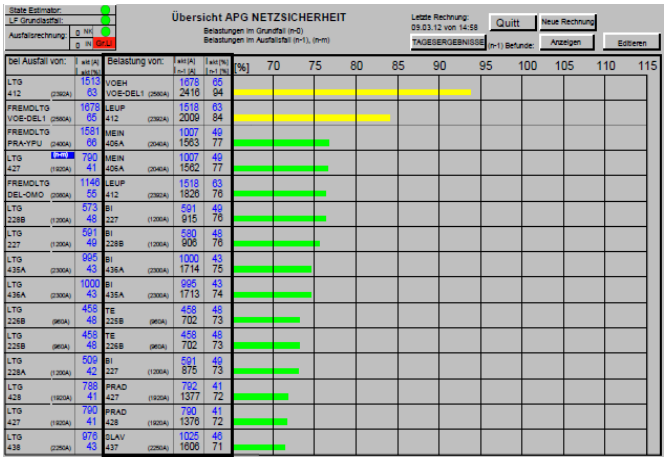
Article 10: Congestion and Power Flows Management

- Coordination, forecast, analysis, margins
- Preventive and corrective measures
- Redispatch, also cooperation with DSOs

Chapter 2. Requirements (4/6)

Article 11: Contingency Analysis & Handling

- „Heart“ of the OS NC
- (n-1), Operational Security Limits
- Forecast & measured values
- Observability & Responsibility Area
- Contingency list (int./ext.):
  - ordinary, exceptional,
  - out-of-range
- Common Grid Model
- Re-Synchronisation



Chapter 2. Requirements (5/6)

Article 11: Contingency Analysis and Handling

It‘s mainly about:

(see Supporting Paper)

One goal

“No cascading with impact outside my border”

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 TSO’s decision

Three behaviours

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

2 - “Best efforts” to set-up remedial actions, that is not always possible or sufficiently efficient by one single TSO to cover exceptional contingencies

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

Risk assessment: a concern

Each TSO is only responsible for the operation of its own network. But it is required to inform relevant neighbors 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, to ensure efficiency of operational decisions and remedial actions.

Chapter 2. Requirements (6/6)

Article 12: Protection

- Protection function, changes → mutual information
- System Protection Schemes coordination with primary protection
- Low Frequency Demand Disconnection coordinated with other TSOs and DSOs

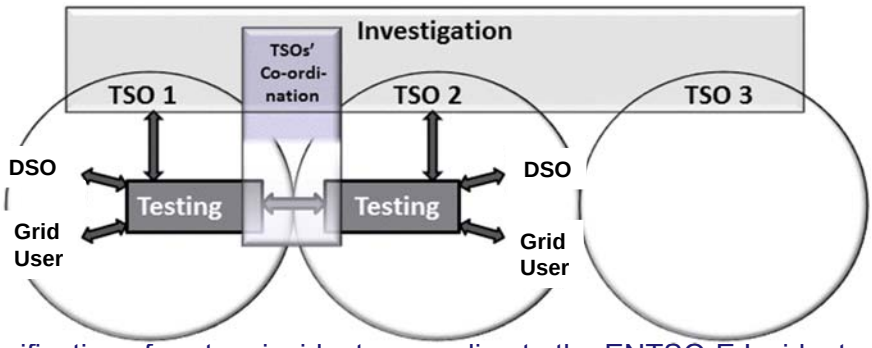
Article 13: Dynamic Stability Management

- Offline or closer to real-time dynamic stability analysis, depending on Stability Limits vs. steady state Operational Security Limits
- Coordinaton with other TSOs
- Methodology for min % of synchronous generation (or equivalent …)

Chapter 3. Testing and Investigation

Article 14: Operational Testing, Monitoring & Investigation

- Roles, tasks and obligations of TSOs, DSOs and Grid Users



- Classification of system incidents according to the ENTSO-E Incidents Classification Scale cf. Art. 8(3)(a) der VO (EG) 714/2009

Chapter 4: Data Exchange

Article 16-17: Structural, Forecast, Real-Time Data between TSOs

Article 18-19: Structural, Real-Timel Data between TSOs & DSOs

Article 20-22: Structural, Scheduled, Real-Time Data between TSOs, Interconnection Owners and Generators connected to TSO

Article 23-25: Structural, Scheduled, Real-Time Data between DSOs and Generators connected to the Distribution System

Article 26: Data between TSOs and Generators Connected to DSO

Article 27: Data between TSOs and directly connected Demand

Article 28: Data between TSOs and Demand connected to DSO

Chapter 5: Training

Article 29: Operational Training and Certification

- Training programme, contents, organisation, coordination
- Offline & on-the-job training
- Certification and prolongation of the licence
- Inter-TSO Training and training with DSOs, interoperability
- Exchange of operational experiences with neighbouring and other TSOs

Highlights

- Contents & structure (update)
- Key provisions (overview)
- Stakeholders‘ suggestions so far
- Next steps

Amendments since 1st WS (1/3)

- **Consistency and alignment (and ever again …) of Definitions**
- **Direct references and relation to NRAs where necessary**
- **DSO as system operator & user**
- **Emphasizing the focus is on transmission**
- **DSOs to receive info from TSOs where needed**
- **Methodology for min. (%) must-run sync. generators (or equivalent …)**

Amendments since 1st WS (2/3)

- Strengthening Data Exchange with organizational elements where applicable
- Emphasizing significance of network development and investments for Operational Security
- Coordinated activities with DSOs where necessary: re-dispatch, data exchange / aggregation, testing, etc.
- Emphasized key cross-issues with other NCs
- Developed Supporting Paper, (FAQ in preparation)

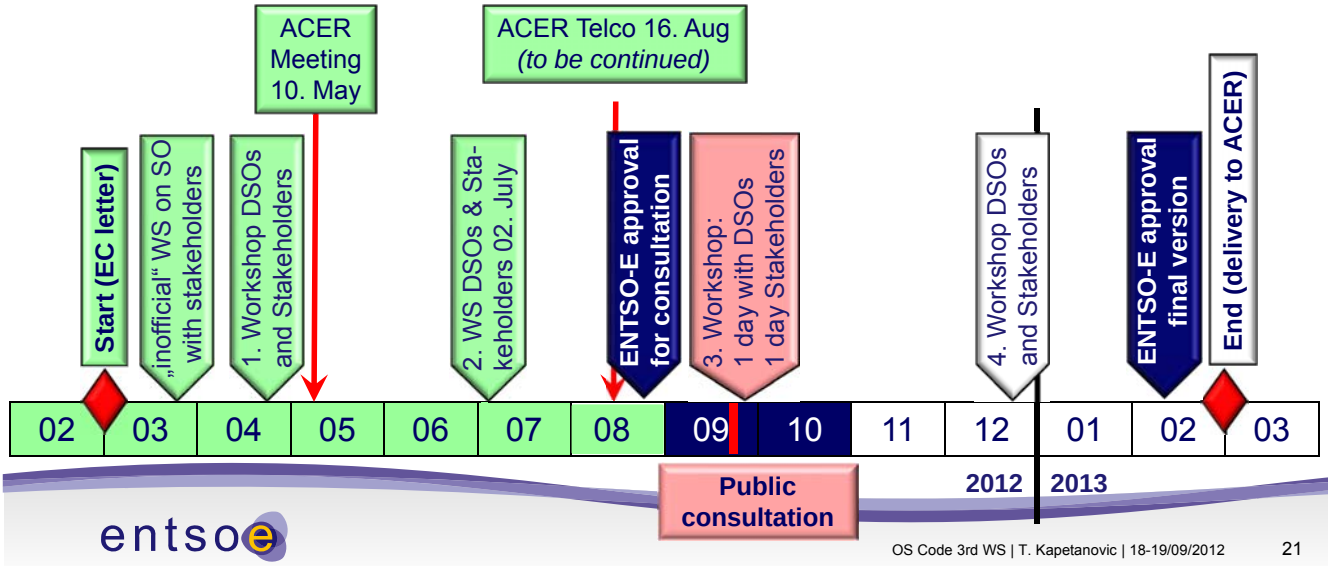
Amendments since 1st WS (3/3)

- „Significant Grid User“ (instead of Grid User) where necessary (throughout the OS NC)
- More precise on responsibilities of ENTSO-E (TSO is legally responsible …) throughout the OS NC
- Amplifying obligations for transparency and non-discriminatory decision criteria
- Transparency of information relevant for the market, confidentiality otherwise (e.g. re-dispatch)
- … and a number of detailed, technical corrections, adjustments, etc.

Where do we stand and what's next

- Public consultation 03.09.-03.11.2012
- Collecting further inputs / needs for Supporting Paper

- Processing of results of Public Consultation in November 2012
- Finalization of OS NC and Supporting Paper
- Final version for 4. WS



Thank you for your attention !