New TSO coordination initiative in Europe


Mavir 1) (Hungary), PSE Operator2) (Poland), Tiwag Netz3) (Austria), transpower stromübertragungs gmbh4) (Germany), Verbund APC5) (Austria), VKW-Netz6) (Austria), Amprion7) (Germany), swissgrid8) (Switzerland), ČEPS9) (Czech Republic), 50Hertz Transmission10) (Germany), EnBW Transportnetze11) (Germany), E-Bridge Consulting12) (Germany), TenneT TSO13) (the Netherlands)

SUMMARY

European legislation demands the Transmission System Operators (TSO) to cooperate more closely, to develop methods and take actions to improve system security of the European transmission grid.

So far most TSOs have developed bilateral agreements for system operations with their neighbours. The current practice shows that such arrangements are not sufficient to cope with the operational challenges due to the very meshed European transmission grid causing more often a possible high impact of the above mentioned phenomena throughout the whole system.

A group of eleven TSOs in Central Europe has set up a permanent TSO Security Panel and started a project to create a common IT Platform for data exchange and performing common security assessments (CTDS). The TSOs agree to improve system security by a more intensive cooperation, to develop common security assessment criteria and to grant an open data exchange (see website [1]).

Especially the continuous development of the international trade and the increase of the low predictable wind power generation lead to unexpected and rapid changes of load flows in the interconnected grids of the concerned TSOs. To cope with these phenomena TSOs require to standardize and to coordinate system security measures.

d.klaar@tennet.org13)
The Security Panel shall be a panel for operational experts to exchange know how about best and new practice and agree on methods in order to ensure a high system security. In the first phase the CTDS shall support the daily security assessment work in the operational planning process of the TSOs.

The objective of the CTDS project is to build up a single common IT-Platform providing functions as follows:
- Receiving operational forecast data from all participating TSOs and adjacent ones
- Merging input data into a unique dataset being input for grid security calculations
- Executing grid security calculations and providing each TSO with relating calculation results
- Enabling additional individual studies on the common IT-Platform for the identification of remedial actions.

The objective of the TSO Security Panel is to improve the management of overall system security by a more intensive cooperation in the field of system operation, focusing on the processes from year ahead till real time by creating a permanent network of operational experts. These experts shall work on improved exchange of information and experience and develop coordinated procedures and remedial actions to ensure a high system security level. The experts have started discussions on each TSO's experienced congestions and possibilities to relieve them. A good proper understanding of the interpretation and use of the security criteria (e.g. "n-1" criterion) together with the knowledge of operational policies and the acceptable risk level is crucial. Both the international rules and regulatory framework (EU Directives, ENTSO-E Operation Handbook) as well as the TSO's own national rules and regulatory framework (Electricity Act, Grid Code) play an important role and determine the degree of freedom for the system operation.

The paper outlines the development process of the common IT-platform and the organisational and technical ideas developed by the TSO Security Panel to further improve the TSO coordination for system operation. Furthermore an outlook towards the future developments of this TSO coordination is described.

**KEYWORDS**

Day-ahead congestion forecast, congestion management, system security, security assessment, regional coordination
SYSTEM SECURITY

System security is the primary goal of the operation of the interconnected transmission system network. In the interconnected transmission system numerous interdependencies exist between the different regional networks. The operation of the interconnected network is based on the principle that each Transmission System Operator (TSO) is responsible for its own network according to ENTSO-E Policy 3 (“Responsibility Area”) [2]. The increasing interference of regional and national systems and the corresponding inter-TSO coordination request more and more coordination on supra-regional level. European legislation demands that TSOs cooperate closely, to develop methods to assess security and take coordinated actions to improve system security of the electrical pan-European transmission system network.

The participating TSOs have agreed to improve system security by a more intensive cooperation in developing common security assessment criteria organizing an open data exchange and performing common security analysis.

Among the range of available and conceivable new remedial actions to relieve congestion those having influence on the market and being coupled with monetary compensation for affected market participants are getting more and more important as topology related measures appear to solve the occurring congestions less and less satisfactorily. This is the case especially from a regional point of view. Today the unsolved question of cost sharing for those measures is the major obstacle for the development of the measures. Therefore in the scope of the TSO initiative a group of experts have been given the task to develop possible cost sharing principles related to cross-border remedial actions intruding the market situation in a given period of time (“costly remedial actions”). This includes a description of criteria for evaluating these cost sharing principles (practical applicability/simplicity, compliance with existing regulatory frameworks, short- and long-run implications) and the evaluation of the cost sharing principles against these criteria.

ORGANISATION

During the past couple of years, especially after the big disturbances in 2003 [3] and 2006 [4] in Central Europe, the pressure for an improved TSO coordination has increased. Furthermore, the increasing introduction of wind energy on the system [5] has made TSOs aware of the necessity of this coordination. TSOs have discussed the several options of system security coordination and came up with two main organizational models: a centralized versus a decentralized approach. The decentralized approach focuses on creating a common control centre which supports the services needed to take care of the regional security. In such a common control centre a team of experts is acting on behalf of the TSOs in the region. One example of such an organizational approach is the Security Service Centre (SSC) that has been organized by the TSOs Amprion and TenneT TSO. SSC though is not a separate legal entity and team members have been recruited from the two TSO organizations themselves. Another example of a centralized approach is Coreso, being a separate legal entity, resurrected by the French TSO RTE and the Belgian TSO Elia.
The TSO cooperation using the CTDS is a decentralized approach: all participating TSOs use common IT-platform and organize their coordinated security assessment work without the necessity of having a physical joint control centre for the TSOs.

The regional cooperation of TSOs does not change the responsibility of each TSO, i.e. each TSO still is responsible for his own control area. The collaboration of TSOs with sometimes legally independent Security Service Centres demands a clearly defined interface in terms of rights and obligations embedded in a legally binding agreement.

The geographical scope of the current initiative of TSOs is illustrated in the figure 1 below.

![Geographical scope of the TSO coordination initiative](image)

**Figure 1: Geographical scope of the TSO coordination initiative**

**SECURITY PANEL**

The TSO Security Panel exchanges know how among the TSOs on the best practices and agree on methods in order to improve and ensure a high level of system security. The TSO Security Panel and CTDS shall support the security assessment work in the common operational planning process of the participating TSOs.

A state-of-the-art overview of the business processes linked to operations was created aiming to get a full picture of:

- Cross-border capacity determination, real-time operation, congestion management concepts
- TSOs' security philosophy for defining and using security limits and thresholds
- The exchange of real-time grid data
- Existing congestions and related remedial actions
- The TSOs' accepted risk levels
- Existing multilateral security coordination procedures.

Shared in-depth analysis on critical events that have occurred is one other important activity that is done by the Security Panel.

**CTDS PROCESS AND FUNCTIONS**

The security assessment process and functions to be supported by the CTDS-System must be compatible with the ENTSO-E Operation Handbook (mainly Policies 3 and 4). The CTDS-System shall provide the TSOs a better view on the entire transmission network system and shall be the basis for a common system security analysis at regional level.

In order to carry out load flow calculation and network security analysis to identify possible congestions or "n-1" violations and remedial actions, it is necessary to exchange relevant data. Hence, one of the main tasks for the TSOs is to organize this data exchange, to agree upon the preparation of the data sets and to ensure the confidential treatment of the data exchange. The TSOs have made an improvement in sharing wind energy forecast information within the region.

The process of congestion forecast is principally split into two steps:

1) Day-Ahead Congestion Forecast (DACF) procedure, based on the network models exchanged by the TSOs in the previous day
2) Intraday Congestion Forecast (IDCF) procedure, based on the information (e.g. network models) exchanged by the TSOs in the current day.

The figure 2 below illustrates the principles of business processes of the CTDS and the Regional Cooperation in the framework of the TSO System Security Cooperation.

![Figure 2: Principle of business processes of CTDS and Regional Cooperation](image-url)
Some important requirements of the CTDS are: it must be open, scalable, flexible and adaptable for future expansions. Furthermore it has to be “portable”, i.e. it has to be sufficiently flexible to be installed at different locations and it has to run under different IT-environments.

The CTDS System is currently under development and will be implemented at the participating TSOs during 2010. The Phase 1 with DACF functionality is scheduled to be operational by the end of June 2010. The Phase 2 with IDCIF is scheduled to be operational by the end of 2010. The CTDS System shall support the daily operational planning process of the participating TSO.

REGIONAL AWARENESS AND ALARM SYSTEM

Next to the CTDS the TSOs also have created a Real-time Awareness and Alarm System (RAAS). The RAAS gives an overview of the following set of each TSOs' important system parameters to indicate a general assessment of the grid situation of a TSO:

- Frequency, in case of network splitting the assignment to over- or underfrequency area is possible
- Setpoint and actual area control value, to assess the control area's balancing situation
- System status indicator (“traffic light”), monitored by each TSO with the possible states being normal, alert, emergency or (partial) black out

In case of a system problem the TSO changes the system status indicator (traffic light) and sends additional emergency information to the participating TSOs. The following figure 3 shows a representation of such a RAAS implementation. The traffic lights are indicated in each control area.

Figure 3: RAAS implementation example
RAAS makes use of the interconnection of the TSOs’ SCADA systems by the Electronic Highway (EH) inter-TSO link (TASE.2 protocol). Hence information exchange can be fulfilled in a simple and fast way using technology dispatchers are familiar with. The bilateral configuration of individual EH connections providing an “anybody-with-everybody” data exchange ensures a high level of reliability. Every three months a common test of the traffic light is performed to secure a high availability of the RAAS.

FUTURE DEVELOPMENTS

It is foreseen that the next step in the TSO coordination is a close to real-time security assessment for the TSOs, possibly supported by optimization strategies and supporting tools in the CTDS. For the RAAS the voltage and frequency per cross-border substation and power flow of each individual tie-line will be exchanged among TSOs as extra parameters.

With the use of the CTDS and RAAS the TSOs' common security assessment and decision making process on relieving security violations on a regional level will be improved. There is still work to be done to improve the TSO coordination and to harmonize the operation philosophies as good as possible.

BIBLIOGRAPHY

[3] Final report of the investigation committee on the 28 September 2003 blackout in Italy (see website www.entsoe.eu)
[5] Final report of the first phase of the European Wind Integration Study (EWIS), 2007 (see website www.entsoe.eu)