P3 – Policy 3: Operational Security

Chapters

Introduction

System safety is the primary goal of the operation of the interconnected network. In an interconnected system there exist numerous inter-dependencies of the networks forming part of the system. In addition, there are impacts attributable to the usage of the system by market players. In an unbundled environment, network operators are not allowed to interfere with market forces unless system safety is at stake.

The operation of the interconnected network is founded on the principle that each partner is responsible for its own network, provided the interference of national system and the corresponding inter-TSO coordination that requests more and more coordination at regional level. In order to give practical application to the basic principle of the interconnection that each TSO is responsible for its control area, one of the purposes of the Operation Handbook is to define the methods of co-operation also in operational situations when factors outside of the control area can reduce the ability of a TSO to operate its system within the operating limits, according to the UCTE rules. To harmonise the operating methods for the interconnected network, UCTE has since the beginning worked out rules, instructions and suggestions, to which the operation of each network has to make reference in order to ease inter-operability.

TSOs are in charge of managing the security of operation of their own networks in a subsidiary way. The most relevant rules for the security of interconnected operation are related mainly to the functioning of interconnections. TSOs cooperatively adapt continuously such common rules for inter-operability to be applied mainly at the borders of their CONTROL AREAS and consequently at the borders of countries / blocks. These rules create favourable conditions for cross-border exchanges induced by network users and by TSOs themselves. All these co-ordinating rules complement any other existing national commitments for network access (legal and contractual) for the transmission networks when they exist. The control of performances of facilities connected to networks remains under the responsibility of TSOs to the extent of their national commitments.

This policy specifies the requirements for operating the TRANSMISSION system to maintain security. Each CONTROL AREA - and TSO - is responsible of procedures for reliable operation over a reasonable future time period in view of real-time conditions and of their preparation. Therefore the N-1 principle has been developed with the goal for each TSO to prevent any propagation of one incident with the meaning of “no cascading with impact outside my borders”. (N-1) principle is then to prevent an emergency condition that appears as a result of a combination of events. Coordination between TSOs contributes to enhance the common solidarity (to cope with risks) resulting from the operation of interconnected networks, to prevent disturbances, to provide assistance in the event of failures with a view to reducing their impact and to provide resetting strategies after a collapse. This co-ordination is intensively developed covering today new aspects related to market mechanisms.

The second edition of this policy focuses mainly on the N-1 rules, which were at stake during the recent European events of 2003 and 2006 *(both were disturbances in normal conditions)* affecting the UCTE power system. The in deep definition of N-1 is based on:
- the risk assessment considered by each TSO,
- the contingencies and their gravity in terms of consequences for the system to be considered in the security calculations whose goal is to detect constraints of network,
- the area to observe the system by each TSO in order to get the best survey of constraints to come,
- the operating limits accepted by TSOs with the minimum risks for the system,
- the remedial actions to cope with and relieve constraints in due time with simulations of their efficiency in advance,
- the strengthened coordination between TSOs to implement such stronger commitments.

We could summarize the philosophy of this new edition of the policy by the following: "TSOs have to be aware (i) of the risk in their own system due to inside or outside contingencies, inform or are informed by neighbors and prepare coordinated appropriate remedial actions in order to avoid uncontrolled cascading with impact across borders" in operational planning and real time. All TSOs shall be aware (ii) that its domestic decisions or actions can have an influence on neighboring systems, therefore coordination is an obligation.

In short, the N-1 principle as described herewith can be summarized as follows:

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.

Current status

This policy focuses only on security aspects in operation and does not deal with long term planning. The commercial rules are out of the scope accordingly. It is to be linked with the Policy 5 “Emergency Procedures”.

Definitions, standards and guidelines are part of the rules.

This policy will replace the document published in 2004

A. N-1 Security Principle (operational planning and real time operation)

1. - Types of Contingencies

Definitions

A1-D1. Contingency. A contingency is defined as the trip of one single or several network elements that cannot be predicted in advance. A scheduled outage is not a contingency. An “old” lasting contingency is considered as a scheduled outage.

A1-D2. Types of Contingencies. The following events to consider contain all elements of the interconnected system at the level of 380/400 kV and above. Additionally all the elements in lower voltage levels of the interconnected system (e.g. 220 kV, 150 kV) having significant influence on the security of interconnected system operation are considered.

A1-D2.1. Normal type of contingency. The normal type of contingency is defined as the loss of a single element. Single elements are as follows:

A1-D1.1.1. a single line,

A1-D1.1.2. a single generating unit,

A1-D1.1.3. a single transformer or two transformers connected to the same bay respectively, a Phase Shifter Transformer,

A1-D1.1.4. a large voltage compensation installation,

A1-D1.1.5. a DC link considered as a generating unit or a large consumer.

A1-D2.2. Exceptional type of contingency. The exceptional type of contingency is defined as the uncommon loss of the following particular elements based on the one hand on the design of the network structure and on the other hand on the probability of the event. The probability of the event can be linked to special operational conditions like storm or maintenance:

A1-D2.2.1. a double line, which refers to two lines on the same tower over a long distance,

A1-D2.2.2. a single busbar, during periods the TSO assesses a significant higher risk of outage,

A1-D2.2.3. the common mode failure with the loss of more than one generating unit, including large wind production, common mode failure of DC links.

A1-D2.3. Out-of-range type of contingency. The out-of-range type of contingency is defined as a failure with very low probability which is not taken into account due to exceeding dimensioning efforts in the single TSO´s network. Out-of-range contingencies are at least the independent and simultaneous loss of two lines, the loss of a total substation with more than one busbar, the loss of a total power plant with more than two generating units, the loss of a tower with more than 2 lines, severe power swinging or oscillations. In case of the occurrence of such an event, the system is in emergency condition and the resulting situation has to be dealt conforming to Policy 5.

A1-D3. Contingency list. The contingency list of each individual TSO is defined as the list of all internal normal and exceptional contingencies considered relevant according to the TSO´s risk assessment. The contingency list includes also the external normal and exceptional contingencies that have to be taken into account by the security calculation due to the potential effect on an element of the responsibility area.

A1-D4. N situation. The N situation is defined as the status of the TSO´s responsibility area that includes outages, but not contingencies. Hence the N situation takes into account all the forecasted outages and known damages of network elements.

A1-D5. N-1 situation. The N-1 situation is defined as the status of the TSO´s responsibility area after an event defined in the contingency list. Considering N situation (that includes already K elements in outage) and L network elements switched off resulting from an event of the contingency list, the N-1 simulation regards these K elements as already out of operation and simulates the loss of these L elements, all together resulting in a "N-L" state.

A1-D6. Cascading outages. Cascading outages are defined as the uncontrolled loss of a sequence of additional network elements caused by an initial contingency.

Standards

A1-S1. N-1 principle. Any event of the contingency list (normal and exceptional types of contingencies considered in the contingency list) must not endanger the security of interconnected operation. After any of these contingencies the operational condition within the TSO´s responsibility area must not lead to the triggering of an uncontrollable cascading outage propagating across the borders or having an impact outside the borders: "no cascading with impact outside my border".

Following conditions must be fulfilled after the implementation of remedial actions:

A1-S1.1. Power flow pattern within security limits. All the current values of the single network elements of the responsibility area remain under control avoiding the impact of cascading effects outside.

A1-S1.2. Voltage deviation. Any contingency of the contingency list does not cause a voltage drop outside acceptable operating limits within the TSO´s responsibility area, which can initiate voltage collapse and cascading outages with impact abroad.

A1-S1.3. Locally limited consequences. As long as the secure operation of the interconnected system is ensured, locally limited and predictable losses of consumption can be tolerated by the TSO within its responsibility area.

A1-S1.4. Limiting cascading effects. If the TSO presumes the risk of a cascading effect with impact outside its borders, it informs the affected neighbor(s). The neighbors complement their respective security computation in order to check the cascading risk at home and to prepare remedies in common.

A1-S2. Coordination for exceptional type of contingency. It is the responsibility of the operator of the concerned network elements to establish the list of the exceptional type of contingency for security calculation based on the likelihood of occurrence of the event and to communicate this list to the neighboring TSOs. Each TSO selects these exceptional contingencies based on the respective risk assessment by itself (see P3-A2-S1). Some exceptional events are considered only in case of temporary specific operational conditions, which have to be communicated to neighbors with a view of security calculation.

If a TSO A considers a resulting risk for an exceptional type of contingency for elements located in the area of TSO B not considered in the contingency list of TSO B, both TSOs reconsider together their contingency lists.

A1-S3. N-1 security calculations. Each TSO has to perform N-1 security calculations to assess the effects of contingencies on the responsibility area concerning load flow and voltage pattern.

A1-S3.1. Preconditions. For N-1 security calculations each TSO must refer to the N situation.

A1-S3.2. Calculations in the operational planning phase. The N situation has to be determined by load flow calculations on the basis of adequate forecast datasets[1]. Each TSO has to perform N-1 simulations for all the contingencies of the contingency list.

A1-S3.3. Calculations in real time operation. The N situation has to be determined by state estimation on the basis of measurements and topology. Each TSO must perform an automatic N-1 simulation for all the contingencies of the contingency list in real time.

A1-S3.3.1. **Frequency of calculation.** The automatic N-1 simulation must run periodically, at least every 15 minutes in real time.

A1-S3.3.2. **Additional N-1 calculations**. The TSOs must perform additional N-1 simulations prior to the application of important topology changes by manoeuvres (opening line, opening bus-bar) or after a relevant unexpected change of topology or a significant shift of the generation pattern (e.g. units tripped or out of operation).

A1-S4. Cascading effects. Each TSO has to be aware of possible cascading effects as a result of security calculation.

A1-S4.1. Identification of cascading outages. The TSO has to assess the results of its N-1 security calculation in respect of triggering a cascade propagating till the boundary of its responsibility area.

A1-S4.2. Cross border cascade. In the case of threatening neighboring TSOs by external cascading outages or by the abroad impact of internal cascading outages the originating TSO must inform the possibly affected neighbors. Thereby the originating and the possibly affected TSOs have to check the impact of the cascade commonly.

Guidelines

A1-G1. Exceptional contingency list. The exceptional contingency list should be updated at least yearly and in due time after the commissioning of a new element or a long term change in the network structure. The related description of new elements or topology changes should be provided accordingly.

A1-G2. Common understanding for contingency simulation. In order to have the same risks level appreciation, TSOs should define at regional level common rules for contingency simulation.

[1] (E. g. DACF)

A. N-1 Security principle (operational planning and real time operation)

2. - Regional Approach - Observability Area Determination

Definitions

A2-D1. Responsibility area. The TSO is responsible for the secure operation (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.

A2-D2. Influence factor. The influence factor is a numerical value used to quantify the highest effect of the outage of an external network element on any internal network branch. The worse the effect, the higher the influence factor value is.

A2-D3. Contingency Influence threshold. The contingency influence threshold is a numerical limit value against which the influence factors must be checked. The outage of an external element with an influence factor higher than the contingency influence threshold is considered having a significant impact on the responsibility area. The value of the threshold is based on the risk assessment of each TSO.

A2-D4. External contingency list. External elements with a contingency influence factor higher than the contingency influence threshold are considered as part of the external contingency list.

A2-D5. Observability influence threshold. The observability influence threshold is a numerical limit value against which the influence factors must be checked. It is used for the determination of the size of the external grid to be taken into account in the security calculation models, so that the impact of the external contingency list on the responsibility area is properly represented. The observability influence threshold is equal or lower than the contingency influence threshold.

A2-D6. External observability list. External elements with an influence factor higher than the observability influence threshold are considered as part of the external observability list. The external observability list includes all the elements of the external contingency list.

A2-D7. Observability area. The branches defined by the external observability list and their terminal buses may not constitute a fully connected consistent external network. Thus they may need to be completed with additional network elements to obtain the consistent observability area, which is implemented in the SCADA system. The observability area includes the responsibility area.

A2-D8. External network. The external network is defined as a network, which is operated by another TSO.

A2-D9. Network branches. Every single line and transformer, that is represented in the network calculation model, is called a network branch.

A2-D10. Network elements. The notion of network element refers to any network branch plus busbar couplers, generators (including pumps), voltage compensation installations, busbars, AC/DC and AC/AC links.

A2-D11. Adjacent and neighboring systems (TO MOVE TO UCTE GLOSSARY). For a TSO an adjacent system is a system directly connected to its own system by tie-lines. A neighboring system is related to the TSO´s observability area, geographically close to its own system; the TSO responsible of that system is called “neighbor”.

Standards

A2-S1. Determination of the external contingency list and observability area.. Each TSO is required to determine the external contingency list and the external observability list related to its responsibility area. External contingency list items must be treated as normal type of contingencies in all N-1 security calculations in all time frames. Additionally exceptional contingencies (double lines, busbars) as announced by a neighboring TSO have to be included by the TSO if it considers them very relevant for risks.

A2-S2. Implementation of observability area. The external network model corresponding to the observability area must be implemented in the SCADA system and its real-time observability by state estimator must be ensured by a proper amount of exchanged online data.

A2-S3. Determination method. The method of determination of the external contingency list and of the external observability list must be based on numerical network analysis. Each TSO can select the most suitable method, but the results must be general enough to be valid in all operating conditions (operational topology changes, maintenance outages, seasonal limits, etc).

A2-S4. Frequency of determination - Co-operation of TSOs. Each TSO must perform the determination of the external contingency list and the observability list at least once a year, and additionally at any time when there is a major change in the network (a new branch is added, an old branch is reconstructed or decommissioned, etc).

A2-S4.1. Data base. The UCTE reference case is due to be used as a basis for the determination of the external contingency list and the observability area.

A2-S5. Information exchange with neighbors related the external observability list. Each TSO must inform the related neighbors about the content of its external observability list.

A2-S5.1. Abroad consequences of grid extensions. Due to the normal evolution of the structure of the neighboring networks (e.g. commissioning of new elements), when a change of configuration occurs, the neighboring TSO reciprocally informs the TSO of such an evolution in order to ease the update of its external observability list and its SCADA system.

A2-S5.2. Abroad consequences of TSOs decisions in operational planning and in real time. In case of changing the network configuration for network branches included in the external observability list of neighbors (e.g. outage of elements, double busbar operation) or major changes of generation pattern, the TSO must inform in due time and firstly in the operational planning phase its affected neighbors[2]. If needed corresponding measures have to be coordinated to prevent counter-effects in neighboring networks.

A2-S6. Data provision. The TSO has to provide its neighbors in due time with all needed information for adequate simulations.

Each TSO must provide the real-time telemetry and the network characteristics to its neighbors that is necessary for the neighboring TSOs to have a sufficient external network model of the observability area for the state estimator and for the N-1 security calculations. This implies among others all data related to switching status, active and reactive power flows, voltage, injections and loads, tap changer position of transformers.

Guidelines

A2-G1. Best practice. It is suggested that TSOs use one of the methods described in the Appendix or any equivalent one for the determination of the external contingency list and of the external observability list.

A2-G2. Risk of losing external telemetry. The loss of the external telemetry and topology status should not prevent the TSO from monitoring the N-1 principle in real time in its responsibility area for its internal contingencies.

A2-G3. Step by step implementation of the observability area. For TSOs who need to increase significantly the representation of external network in real time, they should consider a step-by-step approach by reducing the thresholds of the influence factors

[2] In case of changing outage scheduling and of capacity assessment, TSOs refer to Policy 4.

(based on their risk assessment philosophy) leading to the stepwise expansion of their observability area.

A. N-1 Security Principle (operational planning and real time operation)

3. - Operational limits

Definitions

A3-D1. Permanent Admissible Transmission Loading (PATL). The Permanent Admissible Transmission Loading (PATL) is the loading in Amps, MVA or MW that can be accepted by a network branch for an unlimited duration without any risk for the material.

A3-D2. Temporary Admissible Transmission Loading (TATL). Some TSOs use a Temporarily Admissible Transmission Loading which is the loading in Amps, MVA or MW that can be accepted by a branch for a certain limited duration.

The TATL can be defined in different ways:

- as a fixed percentage of the PATL for a given time (for example, 115% of the PATL can be accepted during 15 minutes),
- several specific couples (TATL; Duration) are calculated for each line taking into account its particular configuration and conditions of functioning (for example, it can be defined a TATL acceptable during 20 minutes and another one acceptable during 10 minutes).

Such a definition of TATL can depend on the initial operating conditions of the network element (sag situation of a line).

A3-D3. Tripping Current (TC). An ultimate intensity, called the Tripping Current without delay (TC), is defined as the threshold the line will trip without any possible remedial actions. The tripping of the network element is ordered by protections against short circuits or by overload protections, but in any case, the activation delay of these protections is not compatible with the reaction delay of an operator (less than one minute).

A3-D4. Overload. The overload of an element means that its PATL is exceeded.

A3-D5. Seasonal adaptations. The PATL - and TATL where applicable - of each network element can change depending on the season and/or on the weather conditions. When the seasonal adaptation is implemented, the tuning is changed at least for the winter and the summer periods. Intermediate regimes can also exist.

For some TSOs, a system to follow-up the real time weather conditions (temperature, wind speed and direction, sunshine, etc.) can exist and it can lead to adapt in real time the operating limits of the network elements.

A3-D6. Voltage ranges for security calculations and in real time.

A3-D6.1. Normal voltage ranges.

The normal voltage ranges for operation are specified through contracts with customers and agreements with Distributors, grid codes, power quality standards (declared supply voltage value and the accepted variation range around this value or thresholds).

A3-D6.2. Exceptional voltage range.

Exceptional ranges of voltage are those related to voltage values (out of the limits of the normal voltage range) that are compatible for a limited time duration with the rating of the equipment, the normal operation of protections, the transformers equipped with on-load tap changers, the auxiliaries services of generator, the electronic power devices.

A3-D6.2.1. **High voltage conditions.**

Referring to the rating of the equipments, a voltage too high can lead to accelerated ageing or the destruction of the equipment.

A3-D6.2.2. **Low voltage conditions and critical voltage.**

A too low voltage can disturb the normal operation of some protections and transformer equipped with on-load tap changers, electronic power devices or can affect the behaviour of the auxiliaries of generation units.

A3-D6.2.3. **Voltage collapse.** For each operational situation there is a maximum active power that can be transported through the network. This point is called the critical point and represents the point beyond the system collapses. This point is also characterized by a critical voltage value. Close to the critical point, small increase of load implies a serious drop in the voltage level of the network.

Standards

TSO commitments for operational security

A3-S1. Transmission loading security in N situation. In normal operation (N situation), any network element is operated below the Permanent Admissible Transmission Loading. If not remedial actions are immediately required.

A3-S1.1. Temporary over-loads in N situation. For some particular network elements (for example, cables or transformers) or for some particular circumstances (for example, radial operation), it is admitted to overpass the PATL in normal operation (N situation) for a known in advance temporary duration. In case of operating an element of the external contingency list of the neighbor in temporary overload, the concerned adjacent TSO has to be informed.

In that case, the overload conditions (respect of the TATL and its allowed duration) have to be respected and if not, remedial actions are immediately required.

A3-S2. Overloads in N-1 situation (simulation). Considering the loss of a network element (N-1 situation) overloads on impacted network elements are admitted only if remedial actions are available as to get back any overloaded network element below its respective Permanent Admissible Transmission Loading PATL.

A3-S2.1. Violation of TATL. If the allowed time corresponding to a given TATL is violated due to a lack of curative remedial actions, the branch is due to be considered as tripped in the network calculations.

A3-S2.2. Instantaneous tripping in N-1 simulation. It is admitted to overpass the TC of a network element after a N-1 simulation exclusively if there is no uncontrolled evolution for the overall system (no cascading tripping, no voltage collapse, no loss of synchronism).

If the N-1 simulation indicates an uncontrolled evolution or cascading effects with impact outside the boundaries, preventive remedial actions are mandatory to come back to an N-1 secure situation. TSO informs its neighbors as soon as the danger of over-passing is detected and no remedial actions are available to avoid it.

A3-S3. Voltage security. At any time, in N situation, the voltage level at any node has to be kept within the normal (contracted or agreed) voltage ranges. In N-1 situation, the voltage level can move temporarily to exceptional ranges under the condition of the existence of remedial actions to go back to the normal voltage range.

A3-S4. TSOs Information sharing.

A3-S4.1. Tie-lines operating conditions. The information on values of PATL, TATL or couples (TATL; Duration), overload conditions (acceptable duration of overload), and TC of tie-lines must be shared with adjacent TSOs. Mutual information must be agreed and implemented. In case of settings changes TSO has to inform the adjacent TSO on the new values.

A3-S4.2. Co-ordination between TSOs at the boundary.

A3-S4.2.1. Tie-lines operational limits. The operational limits (PATL, TATL and TC) on tie-lines to be taken into account are the most restrictive values between the two respective TSOs.

A3-S4.2.2. Synchronising equipment settings. TSO is obliged to inform the neighboring TSO about the settings of the synchronising equipment for switching supervision installed on tie-lines (voltage phase angle difference, voltage module difference, frequency difference).

A3-S4.2.3. Protection system settings. The settings of protection systems for tie-lines have to be co-ordinated between TSOs. Therefore TSO is obliged to inform in advance neighboring TSOs of the settings of protection systems and of changes in operating conditions of tie lines.

A3-S5. TSO Commitments for Alarms. Implementation of Alarms in N situation. In real time in the N situation alarms are generated for different operational thresholds in order to draw up the attention of the dispatcher when the loading or the voltage has reached a certain value ruled by an operational procedure. When the real time measurement of the loading or the voltage of a network element has over-passed this threshold, the corresponding alarm is displayed on the screen of the dispatcher and can activate a bell in the control room. Alarms are generated at least for each tie-line and each 380/400 kV line.

A3-S5.1. Alarms related PATL. TSOs define at least one alarm as to draw up the attention of dispatchers when the loading of a network element has reached a value near or equal to its PATL in N state.

A3-S5.2. Alarms on voltage. An alarm is generated, if the maximum voltage level is reached at one node of the system, at least at the boundary substations. An alarm is generated, if the minimum acceptable voltage level is reached at one node, at least at the boundary substations.

A3-S6. Information provision on constraints generated by N-1 security calculations. Following the automatic N-1 security calculation, a list of constraints generated by N-1 security calculation is due to be available when the pre-defined limits regarding loading and/or voltage are exceeded on any network element in the simulated N-1 situation.

Guidelines

A3-G1. Alarm on voltage resulting from N-1 security calculations. After an N-1 computation, an alarm on voltage can be displayed in case of pre-determined thresholds reached. The activation of a bell is possible too.

A3-G2. Voltage Phase angles.

A3-G2.1. Calculation. TSOs can consider the voltage phase angle difference in their security calculations.

A3-G2.2. Monitoring. When opening important transmission lines or tie-lines TSOs should maintain the system in such a state that the re-closing will be possible when needed keeping the voltage phase angle differences in the accepted ranges. In emergency situations (Cf. Policy 5), TSOs do their best to keep relevant conditions of operation to ensure in the fastest way the re-closing of lines e.g. with a view on re-synchronising the split system.

A3-G3. Reclosing by synchronizers (PSDs).

Depending on the existing grid condition the postponement of reclosing can be preferable as to by-pass the PSD when more favourable operating conditions (exchanges programs, pattern of generation, load evolution, etc.) are expected.

A. N-1 Security principle (operational planning and real time operation)

4. – Remedial actions

Definitions

A4-D1. Remedial action. Remedial action refers to any measure applied in due time by a TSO in order to fulfil the n-1 security principle of the transmission power system regarding power flows and voltage constraints.

A4-D1.1. Preventive remedial action. Preventive remedial actions are those launched to anticipate a need that may occur, due to the lack of certainty to cope efficiently and in due time with the resulting constraints once they have occurred.

A4-D1.2. Curative remedial action. Curative remedial actions are those needed to cope with and to relieve rapidly constraints with an implementation delay of time for full effectiveness compatible with the Temporary Admissible Transmission Loading. They are implemented after the occurrence of the contingencies.

A4-D2. ASAP. After the occurrence of the first contingency and the implementation of the already prepared remedial actions, if the TSO is no more N-1 compliant with a view of the next contingency to come, it implements remedial actions immediately to be effective as soon as possible (ASAP). The notion of ASAP is related to the delay of remedial actions implementation to come back to a new (N-1) secure situation after the occurrence of a first contingency to cope with the following (second, etc.) contingency to come[3]. The state of ASAP can last from some minutes to several hours. ASAP is not related to the first contingency. During the state of ASAP, the system is put at risk.

Standards

A4-S1. Application of remedial actions. Each TSO must prepare in advance remedial actions by its own or in a coordinated way with neighboring TSOs to be implemented in due time to cope with any contingency of the CONTINGENCY LIST.

A4-S1.1. Curative or preventive remedial actions. Curative remedial actions are applied in a time delay compatible with the couple (TATL, duration). When curative actions are not sufficiently rapid, preventive remedial actions are due to be implemented before the occurrence of the related contingency.

A4-S2. Simulation of remedial actions. The efficiency of a remedial action must be checked in advance by (N-1) security analysis and load-flow calculations.

A4-S3. Principle of "No cascading with impact outside my border". TSOs commonly identify, prepare and implement in a coordinated way all possible operational measures and remedial actions (doing their best efforts in accordance with their legal framework) so that the simulated situations[4] based on the contingency lists cannot lead to the propagation of cascading effects outside their borders.

A4-S4. Inter-TSOs principles of remedial actions. Relieving constraints by its own and with neighbors. The TSO facing a constraint is due to trigger relevant actions to relieve the constraint first by its own remedial actions that can be complemented in a coordinated way with its neighbors. In this case coordinated remedial actions are defined between neighbors in order to set up appropriate remedial actions in

[3] Cf. Appendix of Policy 3: "Remedial Actions"

[4] All the situations cannot be simulated in advance, mainly when these refer to emergency conditions (Cf. Policy 5).

common. These actions are due to be implemented without consideration of the originating control area.

A4-S4.1. Regional agreement for the set of remedial actions. For probable constraints impacting neighboring control areas TSOs have to agree in advance with their neighbors in the same region on a set of remedial actions and on related procedures of activation.

A4-S5. Preparation of remedial actions in the operational planning stage. Preventive and curative remedial actions are due to be prepared in the operational planning stage.

A4-S5.1. Remedies are prepared pursuant to the time horizons they are detected: from year ahead, to week ahead and till day ahead.

A4-S5.2. These remedial actions (preventive/curative) have to be previously assessed by numerical simulations in order to evaluate the efficiency of those measures on the constraints.

A4-S5.3. The remedial actions applied by a TSO with possible influence abroad must be checked between all TSOs of the same region in order to prevent counter-effects to neighboring networks. Additional simulations have to be executed.

A4-S5.4. The remedial actions with possible influence abroad have to be agreed by the neighboring TSOs in advance. Therefore information between TSOs is due to be exchanged without any delay as soon as a problem is detected for the real time operation.

A4-S6. Preparation of remedial actions in real time operation or a few hours ahead. In real time, or a few hours ahead, the situation and network configuration is possibly not fully similar to the planned situation studied in the operational planning stage, e.g. in day ahead. TSOs must check that prepared day ahead remedial actions are still well appropriate. They have to adapt previously identified remedial actions in accordance to the system conditions and they must apply them in coordination with neighboring impacted TSOs.

A4-S7. Real time preparation of remedial actions after a first contingency has occurred.

A4-S7.1. After a first contingency TSO duly applies the already studied and prepared curative remedial actions identified in previously security assessments in a delay of time compatible with the triggering delay of the protections and with the Temporary Admissible Transmission Loading (TATL). TSO checks its resulting N-1 situation.

A4-S7.2. For any new constraint to potentially occur, TSO must define a new set of available remedial actions to cope at the best with this new potential [Ň-1] case and apply them immediately to be effective ASAP. The delay of ASAP has to be announced to neighbors.

A4-S7.3. If the new N-1 simulation highlights the risk of propagation of cascading effects with impact in neighboring grids, neighboring TSO has to check the situation, inform its neighbors and must prepare common remedial actions in a coordinated way.

A4-S7.4. In case of lack of internal remedies efficient in due time, the TSO launches alarms to neighbors calling them for help (Cf. Policy 5).

Guidelines

A4-G1. Possible remedial actions. The following list of reference actions that is not exhaustive, can be mixed depending on operational conditions, in planning stage or in real time, the order not being compulsory. It is recommended that the choice of the remedial action should be geared to the minimum impact on the market.

A4-G1.1. Coordinated topology.

A4-G1.1.1. **Change of topology at home.** TSO has first to consider topology changes at home when constraints appear in its domestic network.

A4-G1.1.2. **Call to neighbors to change topology abroad.** If the topology change at home is not considered sufficient in the security calculation firstly, TSO calls for adjacent TSO to check other possible changes of topology.

A4-G1.2. TSO calls for changes of topology abroad after providing to its neighbor the new domestic topology.

A4-G1.3. Modification of the cross-border flow by using Phase Shifter Transformers (PST). TSOs should develop specific procedures to operate in a consistent way the Phase Shifter Transformers in order to control the cross-border flows and limit loop flows to some extent.

A4-G1.4. Coordinated redispatching to relieve constraint at boundary.

A4-G1.4.1. **Redispatching of generation at home**

At the same time of the implementation of possible topology changes at home or abroad, if the constraint appeared in its domestic network is not securely relieved, TSO changes its pattern of generation by redispatching. That shall be checked ex-ante by security calculation.

A4-G1.4.2. **Coordinated cross-border redispatching.** Call to neighbors to change generation pattern abroad.

If the measure of redispatching at home is not considered sufficient in the security calculation, the TSO calls for neighbors to check other possible changes of generation.

TSO calls for changes of generation abroad after providing to its neighbor the new domestic generation pattern.

A4-G1.5. Reduction of exchanges to relieve constraint at boundary.

A4-G1.5.1. **TSO to TSO counter-trading (without impacting the market).** If the coordinated topology and redispatching are not sufficient to relieve a constraint at the boundary, TSOs should implement a counter-trading procedure with neighbors to reduce the flows at boundary.

A4-G1.5.2. **Reduction of capacities, (impacting market).** As the last resort the TSO should reduce scheduled programs allowed to the market at one border and thus reduce the commercial exchanges.

A4-G2. Load shedding as the ultimate remedial action. After the first contingency, in case of lack of remedial actions to bring the system back to N-1 secure conditions following the next contingency, manual load-shedding can be the last resort action to be implemented in a preventive way, in accordance with national laws.

A4-G3. Costly and non costly measures rules in TSO to TSO procedures. The specific analysis for non costly or costly, grid-relevant and market-relevant measures is taken by one or several TSO to implement remedial actions. TSOs implement inter-TSOs mechanisms or agreements to launch cross-border-redispatching or counter-trading and to share/clear the related (over)costs.

B. Voltage Control and Reactive Power Management

Introduction

VOLTAGE is a measured physical quantity, which fluctuates as a function of the network state, i.e., grid topology, generation, load, transmission line and transformer loading. These factors may change due to POWER SYSTEM operator decisions and POWER SYSTEM contingencies (tripping of generators or TRANSMISSION components). The VOLTAGE levels are maintained by REACTIVE POWER generation assured by different facilities. Nevertheless, for network security reasons, and in accordance with operational VOLTAGE security rules for N-1 requests (insulation of network elements, functioning limits of automatic transformer tap changers), a control of VOLTAGE is locally needed to maintain the VOLTAGE deviations within predetermined ranges.

VOLTAGE conditions in a high-VOLTAGE grid are directly related to the REACTIVE POWER situation at the system nodes. Depending on their operational state, all generators, LOADs and system components (lines, transformers) are either REACTIVE POWER consumers or producers. The network by itself produces or absorbs REACTIVE POWER depending on the load level through the line and their surge impedance loading sometimes called the “natural power”. To compensate for an excessive CONSUMPTION of REACTIVE POWER, TSOs have to make sure that efficient producers feed sufficient reactive power into the networks in addition to the one produced by other devices installed in the networks or in consumers installations. It can be the case that a TSO network is more inductive than capacitive in normal operation requesting rather more capacitive sources to control the voltage ranges.

Unlike ACTIVE POWER, REACTIVE POWER cannot be transmitted over long distances efficiently, since the TRANSMISSION of REACTIVE POWER leads to an additional demand for REACTIVE POWER in the system components, thereby causing VOLTAGE drops. In order to obtain an acceptable VOLTAGE level, REACTIVE POWER generation and CONSUMPTION have to be situated as close to each other as possible to avoid excessive REACTIVE POWER TRANSMISSION. This REACTIVE POWER can nevertheless be produced in their RESPONSIBILITY AREA or in the vicinity to those of adjacent TSOs. In this last case, specific bilateral agreements should be made to transfer REACTIVE POWER through TIE-LINES.

VOLTAGE control is thus primarily a regional problem, which may involve several TSOs in an INTERCONNECTED SYSTEM. The operating VOLTAGE reference values are: 380 kV or 400 kV and 220kV or 225 kV. These nominal VOLTAGE values 380kV or 400kV and 220kV or 225kV are slightly different depending on country equipment design; 750 kV is an accepted operating VOLTAGE reference level, too.

The aim of the document is to determine the requirements for individual TSOs and in the frame of their cooperation with neighbors needed for a continuous voltage management in compliance with the N-1 security principles.

Definitions

B-D1. Voltage control. The voltage is regulated in a range of values, which guarantees also in N-1 of elements (described in A1-D2.1):

- the compatibility with the rating of the equipment,
- the supply of customers within the contractual ranges of voltage,
- the voltage stability of the power system, i.e. sufficient voltage stability margins for small and large disturbances in the short term and long term.

Different kinds of voltage control are implemented by individual TSOs, based on their own policies.

B-D1.1. Primary voltage control. It is implemented and is active in operation by the VOLTAGE regulators of generating units, which initiate an automatic rapid variation in the excitation of generators when they detect a variation in VOLTAGE across the generator terminals. The corresponding reactive power is activated by automatic devices in a time response less than a few seconds. Other controllable devices, such as SVCs (Static Var Compensators) may also be involved in primary VOLTAGE control.

B-D1.2. **Other (secondary or tertiary) voltage control.** These are implemented within a delay that can vary till some minutes by (i) either control automatic devices within a given zone of the network, or by (ii) manual actions to activate compensation equipments (such as capacitors and shunt reactors) or topology changes (e.g. cable or line opening in off-peak hour).

Standards

B-S1. Individual TSO voltage management

B-S1.1. TSO responsibility. Policies and procedures for VOLTAGE control have to be developed and implemented by each TSO in its respective responsibility area.

For security reasons and in respect of mutual commitments for operational conditions, a continuous VOLTAGE control is needed and co-ordinated by each TSO in order to maintain VOLTAGE variations within predetermined limits in their RESPONSIBILITY AREA.

B-S1.1.1. Each TSO is responsible for managing voltage and reactive power in its own network (responsability area).

B-S1.1.2. TSOs are in charge of coordinating all needed operational actions with their adjacent TSOs and other stakeholders owning installations connected to the transmission network (Distribution System operators and related distribution networks, connected generating units, connected consumers).

B-S1.2. Reactive power resources and reserves

B-S1.2.1. **Rapid reactive power resources and reserves.** TSOs are committed to have available a sufficient reserve of rapid reactive power resources participating to the primary voltage control in order (i) to ensure normal operational conditions with a continuous evolving of load and transits and (ii) to prevent voltage collapse after any contingency of the CONTIGENCY LIST (including contingencies of one large reactive power source: compensation installation or generation unit).

B-S1.2.2. **Other REACTIVE POWER generation/absorption resources.** TSOs have to keep available a sufficient number of other reactive power sources like generators, capacitors and reactors connected to the grid, which contribute to REACTIVE POWER generation or absorption, in order to maintain or get back the voltage in normal ranges after any contingency.

B-S1.2.3. **Information.** Each TSO must have information of the main REACTIVE POWER resources available for use in the TRANSMISSION network of its own RESPONSIBILITY AREA. TSOs shall be duly informed without delay about restriction of reactive power sources.

B-S2. Inter-TSO coordination for voltage management

B-S2.1. Inter-TSOs coordination.

B-S2.1.1. **Common voltage ranges at boundary.** Extensive REACTIVE POWER flows beyond the own consumption of the TIE-LINES are the result of the different voltage levels on each side of the boundary. In order to ensure a safe operation of the SYNCHRONOUS AREA, adjacent TSOs shall agree on common voltage ranges on each side of the border to ensure the continuous voltage control.

B-S2.1.2. **Coordination for voltage and reactive power management**. A co-ordination between adjacent TSOs is needed in order to manage voltage control (primary and other means) and reactive power resources near boundary preventing that individual actions have a contrary effect to the security of neighbors (including border nodes for voltage) in normal operation and in case of disturbances.

B-S2.2. Data to be exchanged. With respect to the observability area, TSOs exchange data on VOLTAGE values and REACTIVE POWER data for the network security analysis and for real-time operation.

Guidelines

B-G1. Switching TRANSMISSION elements. A manual opening/disconnection of transmission lines can be carried out to maintain the VOLTAGE level within normal voltage ranges e.g. during off-peak periods with low load flows.

B-G2. Remote control of on-load tap changers. In networks including transformers equipped with automatic on-load tap changers, the security of operation may be endangered by these devices in case of serious VOLTAGE drops due to the high LOAD and a REACTIVE POWER deficit. The resulting increase in REACTIVE POWER demand may cause a VOLTAGE collapse. Therefore, it is recommended to use remote control devices to stop the action of automatic on-load tap changers.

B-G3. Contracts for ancillary services – Reactive power provision. TSO can have agreements with providers of reactive power resources to get proper, adequate and rapid reactive power resources complying with operational needs for voltage levels within normal and exceptional voltage ranges and in emergency operation.

B-G4. Data to be exchanged. The amount of reserve of reactive power can be exchanged in operational planning (at least in Day ahead) when possible to inform neighbors about the margins still available concerning (i) the reserve of reactive power of generating units and (ii) the equipments of compensation that are available to be connected. Besides (i) and (ii), the neighbors should also be informed about the expected voltage situation at the corresponding border that can be derived from day-ahead reactive planning results.

C. Short Circuit Currents

Introduction

The network is subject to short circuits between phases or short circuits to earth mainly due to critical atmospheric conditions (e.g. thunderstorms, heavy fog in polluted areas). Short-circuit protective devices are installed for all items of equipment (generators, transformers, bus-bars, TRANSMISSION lines) that promptly and effectively disconnect any occurring fault with selectivity. Their functioning does not result in premature tripping with overloads.

The setting and function of the protective equipment is checked regularly. If there are significant changes in operating conditions, the settings of protective devices are immediately adjusted to suit to the new conditions.

Standards

C-S1. Facilities' short-circuit capability. TSO has to operate its responsibility area in such a way that at any node of the POWER SYSTEM, short-circuit currents do not exceed the breaking CAPACITY of all the devices installed in that node, so that insufficient network fault clearing does not lead to cascading outages. TSO has to use an appropriate protective strategy ensuring selectiveness of intervention and backup protection intervention in case of failure of the main protection system in due time to isolate the fault.

C-S2. Corrective actions. In case of the imminent over-passing of short circuit limits, remedial actions shall exist to manage the values within the limits.

C-S3. TSO Calculation. Each TSO has to calculate where appropriate the short-circuit currents at each node of its responsibility area taking into account the contributions of adjacent systems to the short-circuit power.

C-S3.1. Required data. Adjacent TSOs have to provide each others the required data for short circuit calculations.

C-S3.2. UCTE wide data collection. Each TSO has to provide data for the UCTE reference data set used for short circuit calculations.

Guidelines

C-G1. Topological measures to limit short-circuit currents.

C-G1.1. Network opening. In order to limit the short-circuit currents within the interconnected networks, some network loop opening can be achieved at different VOLTAGE levels in putting lines out of operation, with the risk of creating partial networks connected only through a limited number of lines. In case of bus-bar maintenance, manual opening of lines can be achieved for short-circuit current limitations. Choices are done depending on operating conditions.

C-G1.2. Separated bus-bars operation. TSOs operate sub-stations with different nodes (separated bus-bars) depending on the level of short-circuit currents.

D. Angle Stability

Introduction

This sub-policy deals with angle STABILITY issues from the point of view of preserving the synchronous operation of generators. VOLTAGE STABILITY, due to the local character, is not addressed here even if it can be related to the angle stability. Frequency stability, endangered by a sustained unbalance between generation and load, notably after a splitting of the system, is addressed in Policy 5.

Definitions

D-D1. Angle stability: Angle stability is defined as the ability of the synchronous machines to remain connected in synchronism to the power system after being subject to a disturbance.

Two types of angle stability phenomena are distinguished:

D-D1.1. Transient rotor angle stability The transient rotor angle stability is the ability of a machine to remain connected after having suffered a “major” failure e.g. a short circuit at its vicinity.

D-D1.2. Small-signal stability

Small Signal Stability is defined as the capability of an electric power system or a synchronous machine previously in the steady-state to revert to this state following a sufficiently “minor” fault. If no control equipment is involved in this process, the characteristic is described as natural steady-state stability, otherwise as artificial steady-state stability. The instability may be a single swing or oscillatory instability.

D-D2. Critical Clearing Time. The Critical Clearing Time is defined as the longest duration of a fault that does not lead to any generator loss of synchronism in the system or any other inadmissible repercussion for the system.

Standards

D-S1. Preservation of synchronous operation under normal conditions and after a single outage. Each TSO is responsible for maintaining synchronous operation with other TSOs. All TSOs operate their networks in such a way that a loss of transient STABILITY does not extend to other generating units or lead to cascading effects to adjacent TSOs after the loss of a system element.

The loss of any element, according to chapter A, due to any type of failure, must not lead to a loss of transient STABILITY of the connected generators and induce unacceptable consequences for the whole system with regard to the N-1 principle.

Therefore any generator shall have a critical clearing time higher than the fault clearing time of the protection devices installed in the transmission system (Cf. grid codes with the requirements to generators).

D-S2. Transient angle Stability calculation. Each TSO has at its own disposal relevant dynamic models and dedicated software in order to carry out dynamic simulations ensuring transient angle stability in its responsibility area.

D-S3. Damping of power system oscillations (issue of UCTE inter-area oscillation). In case of STABILITY problems due to poorly-damped inter-area oscillations affecting several TSOs, coordinated analyses are required at UCTE level when appropriate in order to check the small signal stability of the whole power system. TSO is obliged to provide data as requested for specific analysis.

Guidelines

D-G1. Critical Fault Clearing Time Calculation. TSO can perform critical three-phase fault clearing time calculations at any point of its network to compare it with the protection system action delays, to ensure sufficient security margins and to adapt it if necessary.

D-G2. Assurance of angle stability. Stability of the interconnected system can be maintained by following measures

D-G2.1. Power swing detectors. In case of loss of synchronism, large power oscillations appear on the system which can be "seen" by classical distance relay as a fault and lead to chaotic and adverse tripping of lines. Power swing detectors provide a power swing blocking function to prevent false tripping. These relays should be installed in the 380 - 400 kV network.

D-G2.2. Automatic Voltage Regulator (AVR) and Excitation System. As the voltage control is a favourable factor to ensure stability margins, the "right" tuning of the AVR is essential for stability issues. Furthermore, over-excitation capabilities are suitable means to increase these margins.

D-G2.3. Power System stabilisers (PSS). Parts of the excitation system control are used for damping network oscillations in the POWER SYSTEM. It is preferable to equip generating units with power system stabilisers, which are able to damp inter-area oscillations**.**

D-G2.4. Setting of excitation controllers. The TSO is recommended to ensure that AVR (Automatic VOLTAGE Regulators) and POWER SYSTEM stabilisers settings on units within its CONTROL AREA meet its requirements.

D-G2.5. Power unit fast valving. Fast valving consists in a fast reduction of the mechanical power supplied to the electrical machine by the turbine in order to enhance the system STABILITY. Large thermal generating units connected to the TRANSMISSION network should be able to perform fast valving.

D-G2.6. Special protection schemes. TSOs can provide automatic devices at appropriate junctions (international or within the internal networks), which split the grid at predetermined points in the network in order to quickly avoid a spread of a loss of synchronism. Such a solution needs to determine a splitting of the system in several "coherent" areas in which the behaviour of generating units is "synchronous". Therefore these specific automatisms are installed at their boundaries where the oscillatory phenomena have the highest magnitude. Whatever, the presence of such devices and their tuning must be communicated to the other neighboring TSOs.

D-G2.7. Emergency automatics. If it is not possible to ensure the system STABILITY with common devices, also in the view of events of low probability but with serious impact on POWER SYSTEM operation, appropriate emergency automatics should be introduced. Emergency automatics can be used to prevent the loss of STABILITY of a generator group in unfavourable conditions.