Appendix 3: Operational Security

Chapters

1. - RISK MANAGEMENT AND LINK TO "N-1 SECURITY PRINCIPLE"

Introduction

The power system reliability is defined as the ability to:
- ensure normal system operation;
- limit the number of incidents and avoid major incidents;
- limit the consequences of major incidents whenever they do occur.

Such a definition permits an active approach to improving reliability. It encourages one to define the unacceptable consequences of incidents, identify the initiating events and define mitigation measures limiting the risks.

In order to ensure the safety of the system, protection must be provided against four main phenomena that may deeply disturb the system or initiate a large scale incident, naming:
- cascade tripping;
- voltage collapse;
- frequency collapse;
- loss of synchronism.

Reliability, but not at any price

TSO must optimize any operational grid situation by looking for the best quality/continuity of the provided services at the best cost plus penalties ratio.

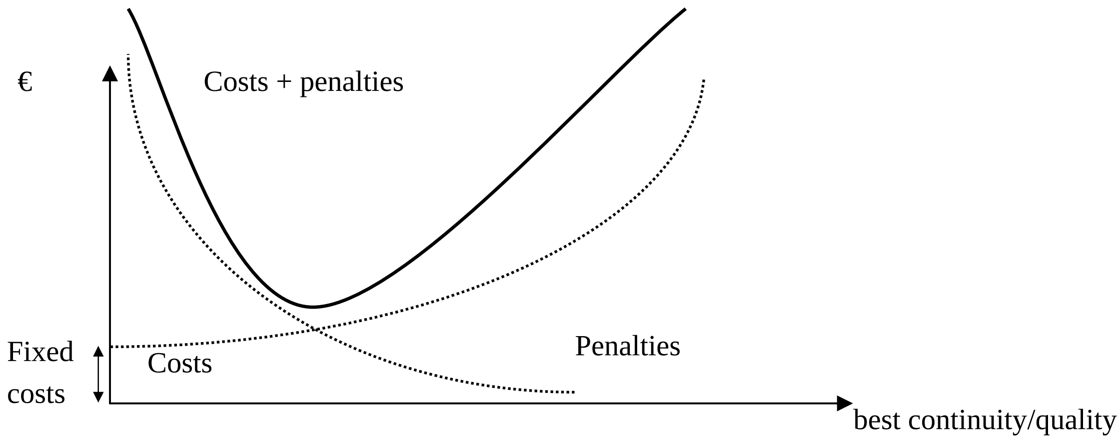


Figure 1: Costs vs. quality

- Cost : expenses generated in order to increase the quality, it reflects the contracted costs such as human resources, tools or preventive actions
- Penalty: non contracted expenses due to a decrease of quality and/or of continuity of the service

At all times, the system operator must do everything that is necessary to ensure that the system remains viable following a hypothetical contingency on the nominal situation leading to the loss of k facilities (substation, line, cable, transformer, load, generation unit, capacitor, reactor, coupling device). Depending on the type of contingency, he can nevertheless tolerate some risk according to a cost-reliability choice.

For example, the outage of a generation unit is one of the most probable events in a network. It should therefore have the lowest consequences on the system. On the other hand, some events, such as the outage of a complete power plant with several units or the loss of a 400 kV substation with more than one busbar, cannot be taken into account due to exceeding dimensioning efforts on the system. Indeed, even if the cascading effect can be effective and the volume of power to be lost can be extremely high, the probability of those events is extremely low.

The TSO must cope with the most probable events by dimensioning its system and defining margins. For rarer events or combinations of events respectively, the TSO may allow a degradation of the system operation, but nevertheless trying to limit the consequences (for example by using automatic load shedding).

Considering the operation of a power system from the point of view of risk management implies the definition of a risk level that should be respected for any kind of events. This risk level is assessed by a reference value of the product “Event probability x Expected loss”. The greater the probability of an event occurrence, the lower the accepted loss. The loss may be defined either by a financial loss or more commonly for a power system in terms of a potential power cut or energy loss.

The following formula quantifies the risk associated to the event i:

$$\boxed{R_i = P_i * S_i \qquad \text{where } S_i = G_i * D_i}$$

- R_i : Risk associated to the event i
- P_i : likelihood of the event i for a given unit of time (namely an hour)
- S_i : Severity associated to the event i, expressed in terms of non-feeded energy. The severity is the multiplication of the Gravity (G_i) and the restitution time (D_i).
  - G_i: Gravity associated to the event i = violation of the operational criteria expressed in non-feeded power (MW).

- D_i: restitution time associated to the event i = time needed to restore the full load if the event takes place

As this risk is given for a unit of time, one can define a mean risk per day by introducing a frequency of exposure. The risk is then defined as :

$$\boxed{R_i = P_i * S_i * f_i}$$

- f_i : frequency of exposure associated to the event i, percentage of the period of analysis where the event will lead to the evaluated severity

As the above definition of the risk is based on the non-feeded energy, it is also possible to determine the cost of this risk :

$$\boxed{C_i = R_i * €}$$

C_i = cost of the risk

R_i = risk as defined above

€ = estimated cost of the non-feeded energy

Based on these definitions, the optimization of the corresponding operational grid situation by looking for the best quality/continuity of the provided services at the best cost plus penalties ratio will lead the TSO to take into consideration all remedial actions having a total effective cost lower than the cost of the risk.

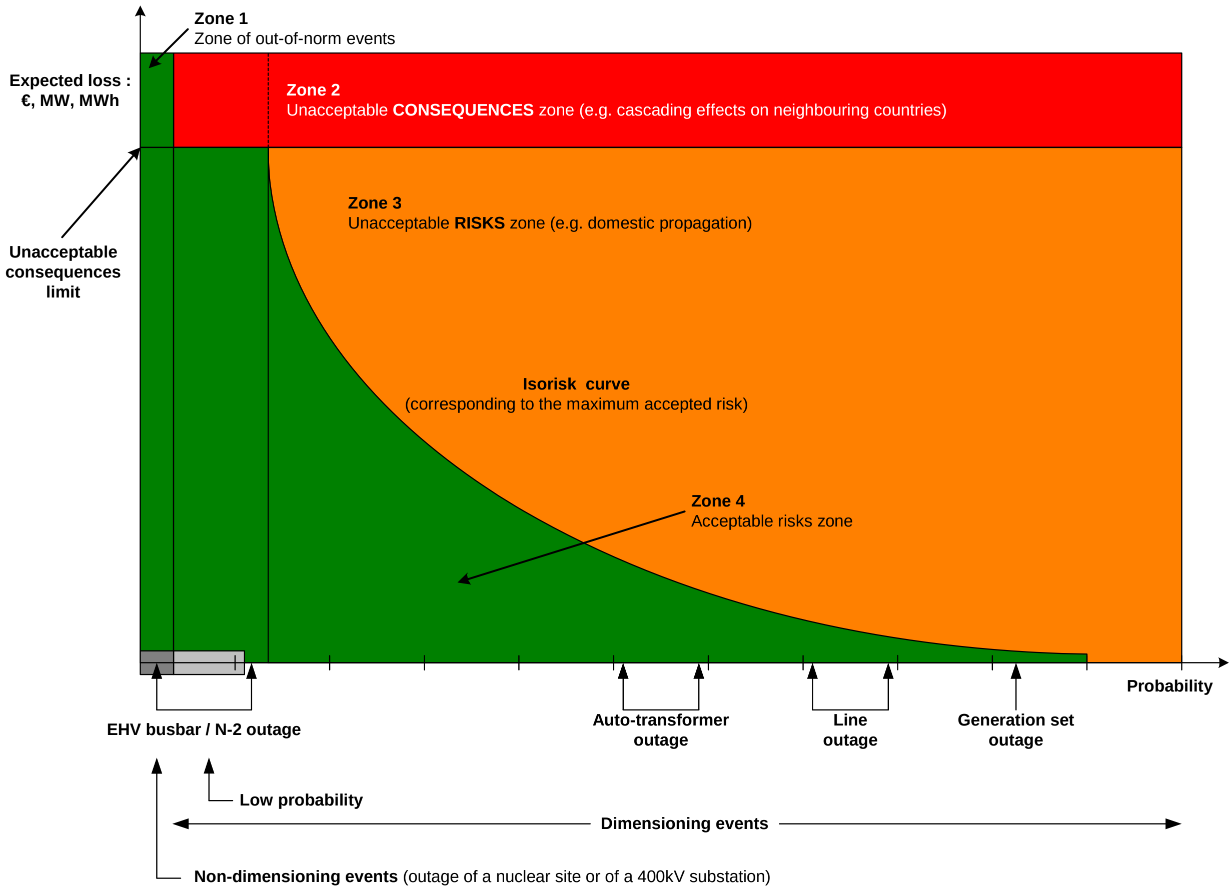


Figure 2: UCTE iso-risk curve

The risk management policy can be summarized in an “Iso-risk curve” (Figure 1). On the horizontal axis the events are located, from the least probable to the most probable. The vertical axis shows the expected loss of each event. Considering a constant risk level as defined above, the potential extent and the probability of the event are linked by the formula:

$$\text{Expected\_loss} = \frac{\text{Risk\_reference}}{\text{Probability}} \quad (1)$$

This definition splits the plan into two main zones (3 and 4). For the most common events (single elements as generation unit, line, tie-line, transformer, large voltage compensation installations), the system should remain inside zone 4, where the risk is acceptable. When going to rarer situation such as common mode failures (combination of single events), the extent has been truncated, lowering therefore the risk. TSO should prefer setting a maximum magnitude of cut for those events (zone 2) in order to protect the system against wider events. Finally, as discussed above, extremely rare events shall have a larger extent (zone 1), as they are not considered for the dimensioning of the system.

Setting the risk reference should take into account any structural problem such as load at the end of an antenna.

To comply with this theoretical point of view, TSOs have first to perform a risk analysis, based on their statistics and experience and define:

- common dimensioning events;
- the probability of those events
- the potential consequences of the events on the network.

From this analysis, TSOs should be able to share a common risk level in the future, defining at the same time a reference point for the reliability of the European system and the required investment to reach it. Due to the different historic approaches for the dimensioning of the power system from a TSO to another it may lead to different risk levels and potentially jeopardize the reliability of neighbouring TSOs.

Remedial actions

Curative and preventive remedial actions are commonly defined. Curative remedial actions are implemented after a contingency in order to quickly relieve constraints on the system. They have to be defined in advance and their efficiency must have been previously proven by simulation. Curative remedial actions are generally defined in operational planning in compliance with real-time operational constraints.

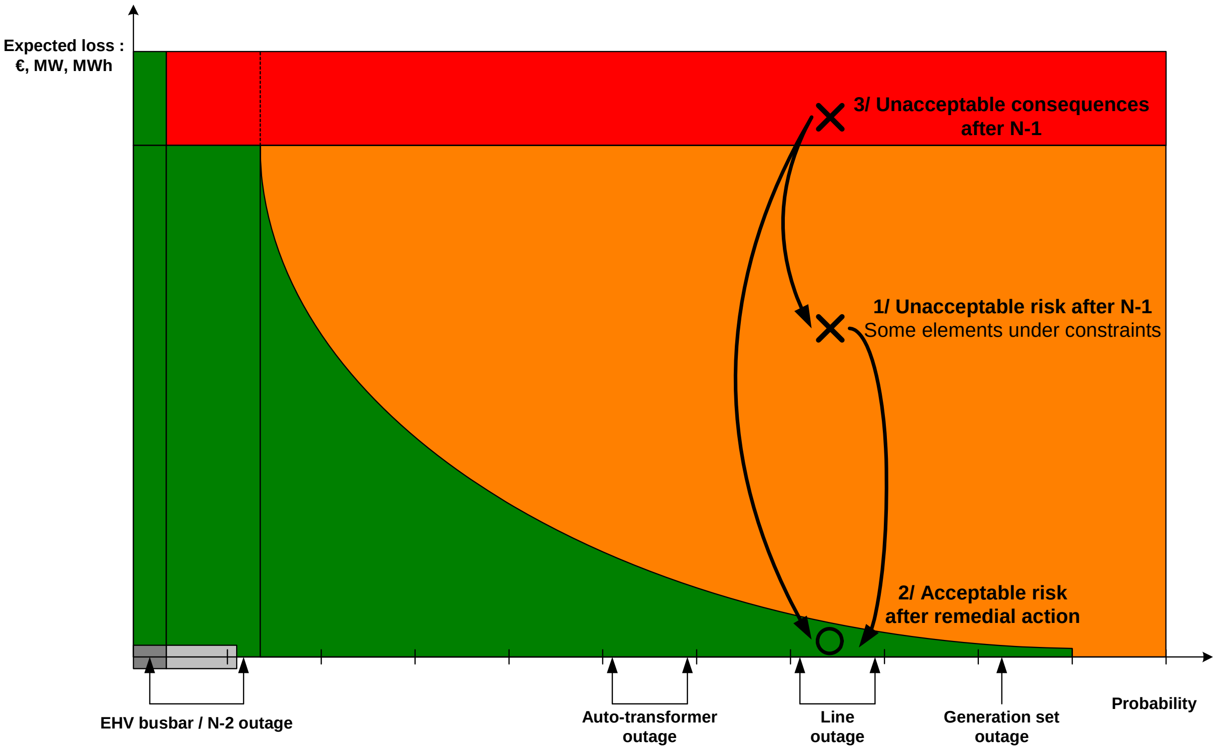


Figure 3: N-1 and remedial action

Figure 3 shows the consequences of the implementation of a curative remedial action on the iso-risk curve. After a line outage, constraints on other elements put the system at risk (1). A curative remedial action should alleviate the system and restore the risk to an acceptable level (2).

Preventive remedial actions on the other hand are decided and implemented in advance. In those cases, curative remedial actions are not efficient or do not exist. Preventive measures have to be taken in order to restore margins on the risk level. For example after a contingency, the system is at risk (1), and a preventive remedial action restores it in (2).

Obviously, combinations of preventive and curative remedial actions are possible, each of them having different consequences on the risk management. For example, in Figure 3, the system is at unacceptable risk level after a contingency (3). A preventive remedial action will restore the system to (1) where curative remedial action will be available, in order to guarantee that after the contingency the risk of the system will be restored to an acceptable level (2).

It is up to the TSO to ensure full efficiency of preventive or curative remedial actions. But it can not be mandatory to cope with the failure of the remedial actions (e.g. failure of devices).

N-1 principle

For the sake of simplicity and to easily put this risk policy into operation, it is usually preferred to turn it into the well known “N-1 principle”. This rule guarantees that the loss of any set of elements of the network is compatible with the operational criteria of the system, taking into account available remedial actions. As some remedial actions (like load shedding, generation redispatching or capacity curtailment) could be very expensive, limitation has to be applied in the usability of these ones, defining implicitly a reference risk level (which could be associated to a maximum power cut for each event). The “N-1 principle” is only a way to assess a given risk policy. Tightening the rule limits the risk but usually requires greater investments.

For example, respecting a N-1 principle without any consequence on the system for the current events would force the system to lie in the dark green area in Figure 4. This rule would be far to much restrictive because this would not allow the loss of a load at the far end of an antenna. Structural limitations must be taken into account in the risk assessment.

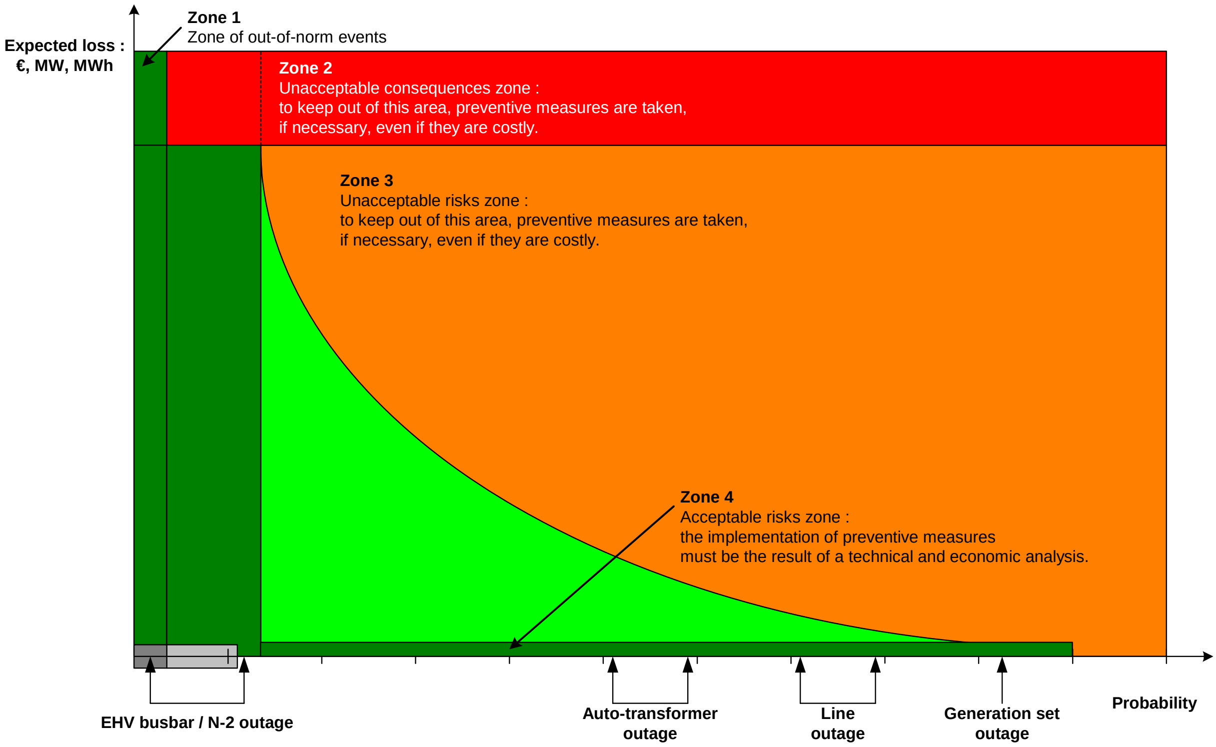


Figure 4: N-1 on current events without any consequences

N-1-1 and ASAP restoration

A critical problem after a contingency is the time needed for the restoration of the N-1 secure state. After the loss of a network element and the application of any potential remedial action, the system should not be at risk if the N-1 rule is enforced. However, nothing guarantees that the system may cope with another disturbance. Remedial actions have put the system in an unconstrained N-1 state but measures have to be taken in order to find a new Ñ state able to deal with other contingencies, respecting an "Ñ-1 rule". Finding this new Ñ may not be easy and sometimes impossible without the lost element. Before getting this new state Ñ, any new contingency is defined as an N-1-1 outage, referring to the past event.

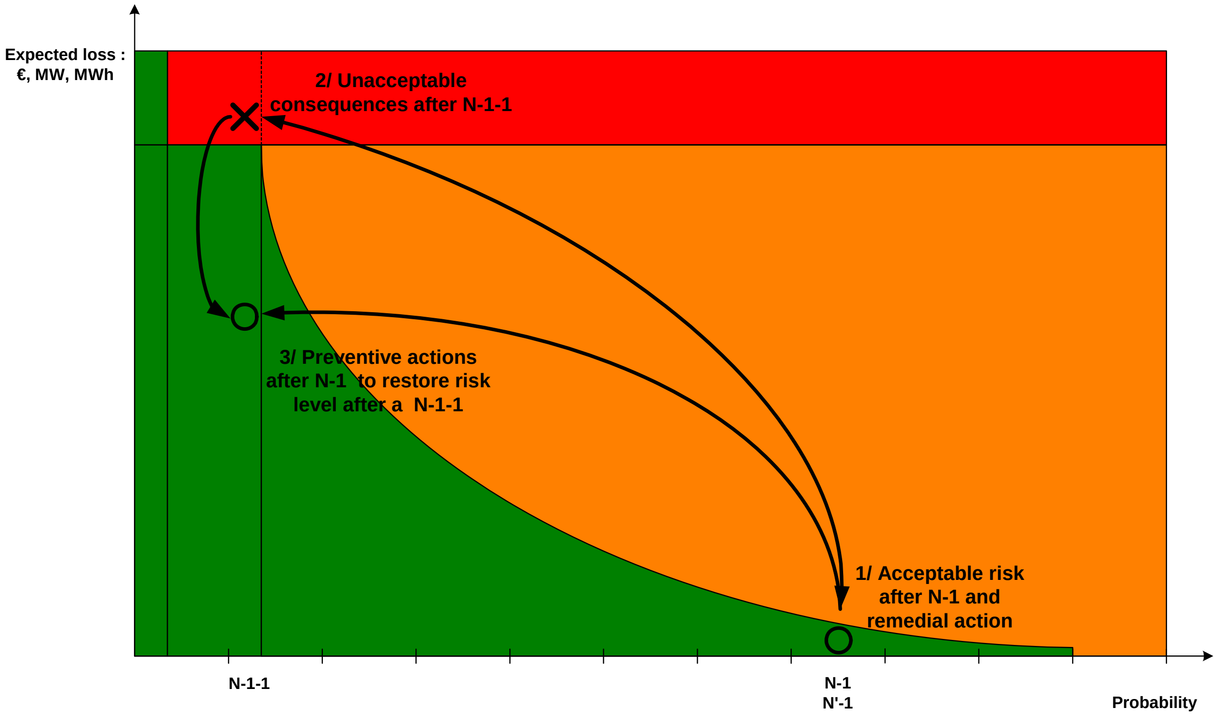


Figure 5: N-1-1

For example, in Figure 5, the first contingency complies with the N-1 rule. Potential curative remedial actions may have been applied and the risk level is under control (1). Operators must then take measures in order to restore an Ñ state or protect the system against another outage with unacceptable consequences (2) by setting preventive remedial actions (3). ASAP restoration means finding an Ñ state for which any new outages would respect the risk level. During this restoration period the system may be at risk.

2. - TYPES OF CONTINGENCIES TO TAKE INTO ACCOUNT FOR N-1 SIMULATIONS

Definition of types of contingencies to take into account - Contingencies to cover

A contingency is defined as the trip of an element that cannot be predicted in advance. A scheduled outage is not at all a contingency. An “old” lasting contingency is considered as a scheduled outage.

“No cascading with impact outside my borders” principle.

The principle to be used is to prevent cascading effects of a contingency with impact abroad: Each TSO simulates the possible cascading effects in order to check

- whether the collapse could be propagated at least till the boundary, given the neighbour is alone the best placed to simulate the progression of this cascading effect at home
- the potential unbalancing of the UCTE system frequency and also the deterioration of voltage for neighbouring TSOs.

In this case the originated TSO informs the neighbours in order they check the situation at home. The originated TSO provides its neighbours with all needed elements for simulations.

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.

Normal type of contingency

The normal type of contingency comprises the loss of a single element, which can be

- a line
- a tie-line
- a DC link
- a unit
- distributed generation of a relevant size like a clustered wind farm, cogeneration, etc.,
- a transformer (including Phase Shifter Transformer)
- a large voltage compensation installations.

Exceptional type of contingency

The exceptional type of contingency comprises the loss of the following elements:

- N-1 double circuit line: A double circuit line refers to two lines on the same tower over a long distance. The consideration of distance is left to the appreciation of each TSO.
- N-1 busbar: The contingency can occur due to the failure of a breaker or internal lack of insulation, fault of protection devices, etc.
- N-2 units (common mode on ancillary services, etc.)

These contingencies are considered by a TSO depending on its own risk assessment in order to prevent cascading effects and to comply with the “no cascading with impact outside my borders” criterion. A few elements can be concerned. Each TSO assesses its list of exceptional contingencies. Exceptional contingencies are computed in security calculations like normal contingencies as being a part of the contingency list.

Out of range type of contingency

The out of range type of contingency comprises losses of elements with a very low likelihood as e.g:

- N-2 lines
- a total substation with more than a busbar,
- a total power plant with more than two units,
- a tower with more than 2 lines,
- severe power swinging or oscillations, etc

They are not considered.

For normal contingencies and exceptional contingencies N-1 simulations are mandatory, including on-line automatic simulation in real time operation.

Day ahead preparation of remedial actions[1] is mandatory as well. 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. Therefore a coordination of remedial actions is necessary if an impact of an outside contingency has been detected by a neighbouring TSO. These remedial actions are to be applied in real time.

The contingency list to be used for N-1 security calculations includes both internal and external events (refer to regional approach issue).

Some TSOs consider one or all of the exceptional type of contingency depending on operational conditions and the structure of the grid.

The Consideration of N-1 double circuit lines depends for some TSOs on the risk for the overall system, on operational conditions (maintenance on one circuit of a double circuit line), weather conditions mainly near real time (snow, storms or hurricanes - speed of wind), on the length of double circuit lines, geographical situation.

The schemes of network configuration have to be exchanged in due time in advance to inform neighbouring TSOs about a particular temporary topology change, in addition to a regular exchange about the normal topology. The real time exchange of data including the status of breaker and switchgears in the substations contributes to this up-date.

Changing the network configuration in a bordering substation can induce the neighbouring TSO(s) to strengthen the security analysis with exceptional types of contingencies. That is the case of the existence of a bordering substation with only one busbar (after outage of the other one), to which a double circuit line is connected[2].

The updating of the exceptional contingency list – subset of the contingency list - should be made regularly (at least once a year) or after relevant long-term changes in operation. The computation should take into account the N-1 principle “No cascading with impact outside my borders”. Each TSO should determine the list of exceptional types of contingency – double circuit lines and bus-bars mainly – to be considered and has to exchange this list and the related description of these elements with all the involved TSOs.

---

1 For remedial actions, one considers two categories:

- *Curative remedial actions are these needed to cope with and to relieve constraints rapidly. They are implemented after occurrence of the constraints.*
- *Preventive remedial actions are those launched in anticipation of the event, due to the lack of certainty to cope efficiently and in due time with the constraints once occurred. These preventive remedial actions are either fully effective before the contingency occurrences due to the high risk for the system or are fully effective after a certain delay of time (e.g. delay of production of a cold power unit).*

2 E.g. case of the Uchtelfangen substation in Germany with the increased risk of N-2 double circuit Vigy-Uchtelfangen (Vigy in France) in case of only one busbar is in operation: in this case strengthened simulations are due to be launched for security analysis due to the risk of severe loop flows through the Netherlands and Belgium. The results have to be compared between affected neighbours.

A specific case for cascading: The loss of bus-bars

First of all it is recalled that the risk assessment is firstly a concern for each TSO for its own network. Each TSO is only responsible for the operation for its own network. But it is required to inform neighbours with relevant information in case the TSO assumes some risks to come from outside and to coordinate actions or in case of operational condition increasing the probability of some exceptional contingencies.

Coping with consequences depends on the regional context with or without transits, that can amplify the consequences of a loss of a busbar. The loss of a busbar corresponds to the loss of N-k elements. In normal operational conditions, the probability of such an event can be considered as quite low. The network has not been designed to cope with these rare cases. It is not affordable to consider a priori an event which could be considered as an “out-of-range” contingency with mandatory - and then very costly - remedial actions in order to prevent all consequences due to the very high cost of this.
But each TSO can have a different approach for the risk assessment, that can be far different from its neighbour being of mutual interest in the bordering substations. Moreover, in some particular operational condition (i.e. maintenance of one busbar), the probability of collapse could increase significantly.

To cope with the “be aware of the risk”-principle, TSOs should monitor the severity of consequences resulting from the loss of a bus-bar in these particular areas based on its own risk assessment. To use the same upper risk approach is the way to prevent cascading consequences: Neighbouring TSOs should simulate the same exceptional contingency, if one considers a risky situation.

The following recommendation affects in particular the situation of maintenance on bus-bars: in case of maintenance on one busbar in a (bordering) substation comprising two bus-bars, the loss of the sole busbar in operation can be very jeopardizing to the system due to the possibly higher probability of the occurrence. Alarms to neighbours should be forwarded in advance.

But to cope with the loss of bus-bars in general is not affordable. TSOs are always committed to do their “best efforts” to limit cascading effects, searching remedies by its own or with assistance of the neighbours at regional level. But for bus-bar failures the consequences to cover are out of range and such a contingency leads to emergency operation.

It is noticed that some grid codes are not in accordance to cover the loss of the second busbar during periods of maintenance of the other one.

At the border between two TSO one can distinguish two cases:

- Case of domestic contingency simulations (e.g. loss of bus-bar at home) The TSO informs its neighbor about the simulated contingency and risky consequences, with remedies available or not. It is recommended that the neighboring TSO simulates the same risk (checking likelihood of cascading effect).
- Case of contingency simulation located outside of one TSO´s area (e.g. loss of bus-bar in an external but close substation – mainly bordering). If a TSO A simulates such a kind of contingency in the neighboring system of TSO B because it considers a risk for its own system (e.g. in a bordering substation), TSO B could simulate the same risk, and provide TSO A with the conditions of operation and to search for remedies (to limit cascading) by its own or with the assistance of neighbors at regional level.

In a coordinated way, the neighboring TSOs could reconsider in depth their exceptional contingency list in order to prevent a cross border cascade (Cf. rule of Policy) and to have a ((i) common level or (ii) common knowledge of risk.

The most relevant remedial actions in case of a loss of a bus-bar are as follows:

- Redispatching and cross-border measures (level of neighbouring TSO assistance) in preventive and curative ways
- Exchange programmes reduction Day ahead (and intra-day when possible)

- Load shedding principles as the ultimate action, depending on the possibilities of the national grid codes

As already stated above there is an obvious link to “emergency operations” in this situation.

Simulating loss of bus-bars would imply further improvements in the data exchange files for security calculations for some TSOs, with a more detailed description of substations.

N-1 security calculations

To prevent converse effects of contingencies and cascading effects with impact outside the borders, each TSO launches N-1 security calculations The aim of N-1 simulations is for each TSO to be aware of the consequences of trips of network elements (as defined in the types of contingencies) and to prepare adequate remedial actions to prevent network constraints (for the normal type of contingencies and exceptional type of contingency and/or cascading situations outside its borders (the risk occurs mainly for exceptional type of contingencies).

TSOs analyze particularly the impact of outages of network elements within the external contingency list on the responsibility area at all planning stages. That means in the operational planning phase by using forecast datasets (i.e. DACF or UCTE reference cases) and in real time operation by online N-1 calculation.

In all cases when a contingency affects neighbouring control areas, involved affected and originated TSOs check together the efficiency of the remedial actions by an additional computation on demand of the affected TSO. The following figure highlights the above described principle for the special case of risks affecting more than one TSO.

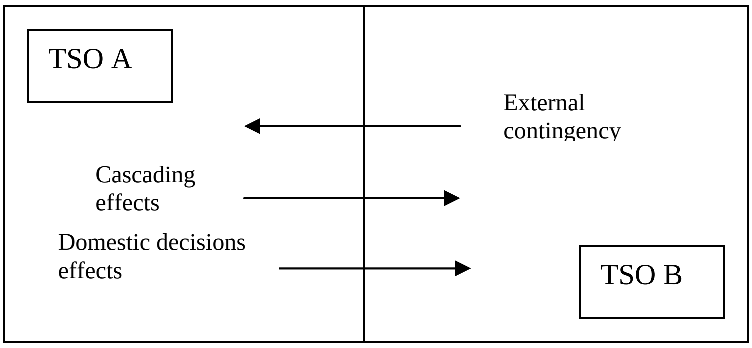


Figure 6: **Risk analysis from inside and from outside of TSO A**

At any operational planning stage or in real time, TSO A simulates risks coming from outside based on the external contingency list.

TSO A informs its neighbours of risk of cascading from inside to outside or of decisions influencing significantly the flows in the neighbouring system. Coordination is required to set-up a convenient set of remedial actions in case best efforts by TSO A firstly to be implemented are not sufficient.

The scope of security analysis is related to the simulation of

- Contingency and constraints of network element
- Voltage patterns

The studies related to voltage phase angles differences are left at present to the discretion of the TSOs. Studies on stability are not in this mandatory scope of N-1 systematic security analysis.

“N situation”

The loss of any network element is studied from a “N situation” reference, which is defined as follows: The reference “N situation” takes into account all the forecasted outages and known damages of the network or generation; considering k elements in outage, it means that the N-1 simulation considers these k elements already out of operation.

Scope of N-1 security calculations in operational planning stage

Each TSO, taking into account the planned outages in the network and the best forecasted demand and generation scheduling available, must simulate all the possible N-1 situations (in accordance with the contingency list). In particular that means:

- Simulations for normal contingencies is mandatory.
- Mandatory simulations for exceptional contingencies are launched based on the subset of exceptional contingencies defined in advance according to the TSO´s risk assessment.
- Out of range contingencies are not simulated .

Scope of N-1 security calculations in real time

a) Mandatory automatic N-1 simulations:

TSO has to perform systematically an automatic N-1 simulation for the normal type of contingency and for the subset of exceptional type of contingency defined in advance in order to detect potential inside constraints and to comply with the “no cascading with impact outside my border” principle.

Each of these N-1 simulations takes place with a periodicity of a few minutes (at least fifteen minutes)

b) Manual N-1 simulations in real time to complement automatic ones:

TSO launches an additional N-1 simulation to confirm the diagnosis of simulations performed in operational planning (and checks mainly the efficiency of remedies) taken into account the new pattern of the network.

TSO launches N-1 simulations for exceptional contingencies based on the subset of exceptional type of contingency defined in advance and on additional ones, for which it presumes to put a risk on the system.

c) Manual N-1 simulations after the occurrence of the first contingency

A new “Ñ situation” (Ñ=N-1 + applied remedies) would have to be redefined after any tripping corresponding to an analysis of a potential Ñ-1 situation to come (see as well chapter on remedial actions).

So the TSO launches immediately a new Ñ -1 security calculation with results to detect new constraints to come; this is carried out without delay after the implementation of the set of prepared remedial actions (for the first N-1).

TSO launches also new Ñ -1 simulations for exceptional type of contingency as above-mentioned in real time.

For the new constraints to potentially occur, TSO studies a new set of remedial actions (in coordination with neighbours if any).

The same continuous process is restarted after any new other contingency, if any.

3. - DEFINITION OF REGIONAL APPROACH – DETECTION OF CONSTRAINTS

General approach

Up to now TSOs have had to monitor the N-1 security approach for their own system at any time through the observation of their own system and some defined but not specified parts of adjacent systems and carry out security computations for risk analysis at any time.

This document focuses on elements of the methodology for the regional detection of constraints upon the interconnected system.

TSO is obliged to monitor the N-1 principle within its own grid including all the tie lines to its neighbouring grids, calling it the RESPONSIBILITY AREA (P3-A1-C1) of the respective TSO.

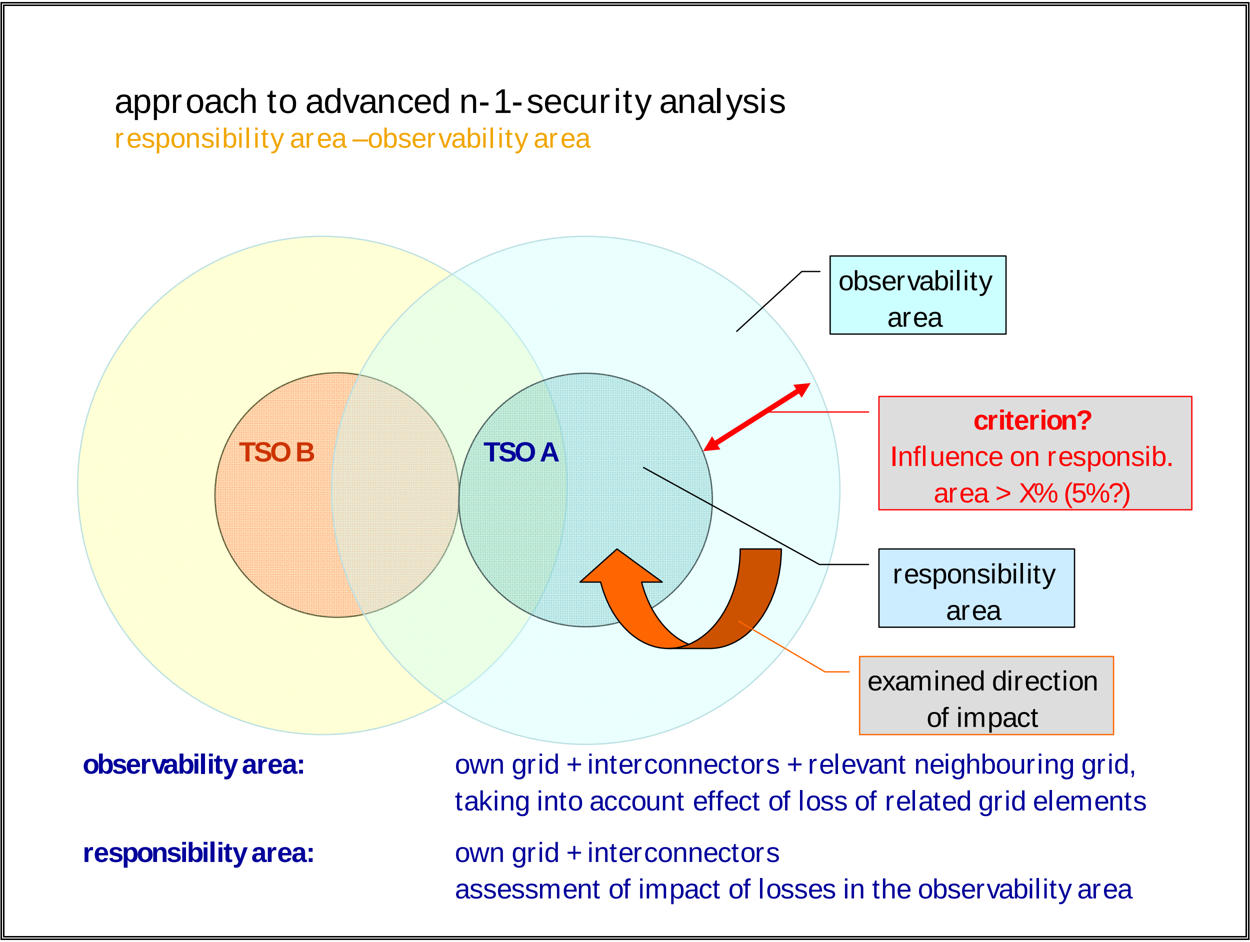


Figure 7: Definitions of responsibility area and observability area

Acknowledging the fact that, due to the increase of interconnections among TSOs the assessment of security is more and more interdependent, the TSO has to take into account the influence of the surrounding grid on its responsibility area.

In the past the regarded surrounding grid resulted from local structures (might be a question of meshing, size and location of the single TSO´s grid within UCTE grid) and historically developed operational needs. It usually comprised the 1st and 2nd loop of the guard rings at the most. The recent developments reveal that the principle of regarding the 2nd loop is not a sufficient criterion of observability as elements beyond might have a major impact as well. As a consequence it could be required to comprise even further elements outside (3rd guard ring or beyond).

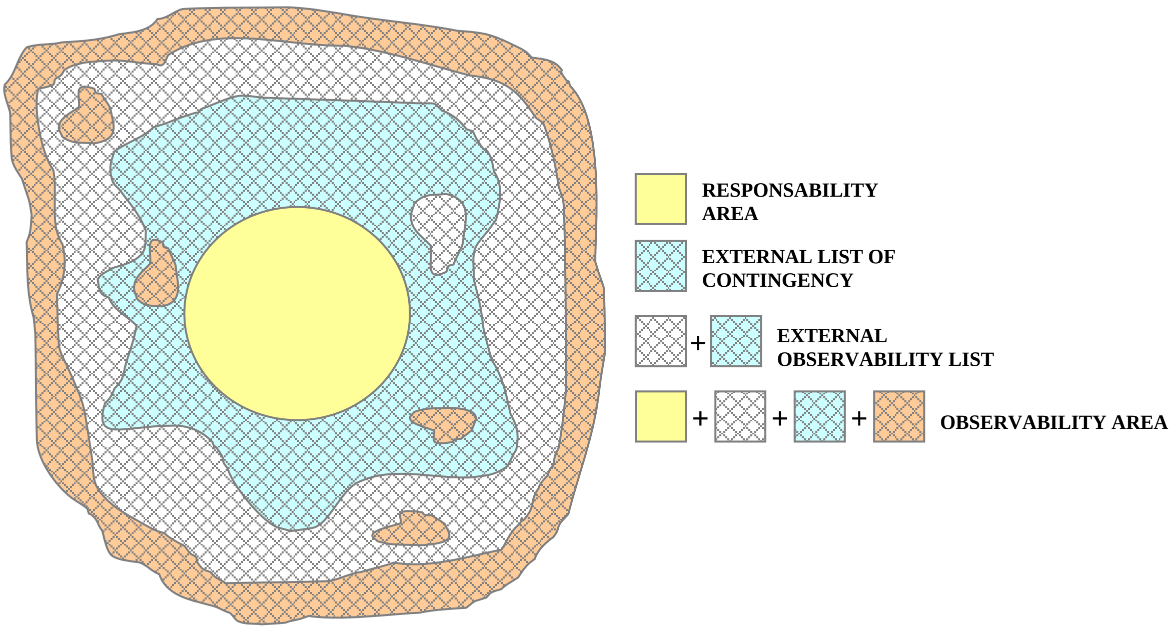
Each TSO is due to analyse periodically, by numerical calculations, the external transmission network with influence on its RESPONSIBILITY AREA. The EXTERNAL CONTINGENCY

LIST (P3-A1-C4) is the result of that analysis and includes all the elements of surrounding areas that have an influence on its RESPONSIBILITY AREA higher than a certain value, called the CONTINGENCY INFLUENCE THRESHOLD (P3-A1-C3).

Each TSO has to take into account the elements of this EXTERNAL CONTINGENCY LIST in its contingency analysis. Therefore the correct solution of the state estimator has to be assured: not only the correct indication (simulation) of the load of network elements in the RESPONSIBILITY AREA near the border in the N situation, but also the correct simulation of the effects of outside outages in the near vicinity on the RESPONSIBILITY AREA.

It is necessary to have an on-line model of the external grid wide enough to guarantee accurate estimations (in the RESPONSIBILITY AREA) when performing the N-1 analysis of the elements of the external contingency list. That means that not only the branches of the external contingency list have to be modelled. Other surrounding branches, with lower influence on the RESPONSIBILITY AREA, have to be part of the model as well, to ensure correct simulations of the effects of abroad outages. All the external elements with an influence on the RESPONSIBILITY AREA higher than a certain value, called the OBSERVABILITY INFLUENCE THRESHOLD (P3-A1-C5), constitute the EXTERNAL OBSERVABILITY LIST (P3-A1-C6). The EXTERNAL OBSERVABILITY LIST could be a non consistent model. For example a certain external line could be part of the observability list meanwhile its neighbour branches are not in this list. Therefore, the model must be completed with additional network elements and some equivalents to obtain the consistent and fully connected OBSERVABILITY AREA (P3-A1-C7), which is implemented in the SCADA system. The OBSERVABILITY AREA includes the RESPONSIBILITY AREA and the external network, so each TSO is able to simulate properly any contingency of the external contingency list when performing the N-1 analysis.

The following graphic illustrates the concepts defined in the previous explanation:



OBSERVABILITY AREA = RESPONSABILITY AREA + EXTERNAL OBSERVABILITY LIST + BORDER AREA + MODEL TERMINATION AREA

Figure 8: Principle design of an online model of the external grid

The inquiry of the tripping of external generators shows important results as well even if the time of the system imbalance is normally limited as the involved TSO will rebalance its system within minutes. Nevertheless mid term effects may be difficult to evaluate as the related remedial actions affecting the pattern of generation are non predictable.

The EXTERNAL CONTINGENCY LIST could be strengthened in specific situations if the neighbouring TSO considers an increase in the potential risk of tripping of certain elements (due to maintenance works in a substation, extreme weather conditions…) or if the topology of the network changes and that implies a modification in the influences of external outages. Therefore coordination is necessary between neighbouring TSOs for proper determination of the EXTERNAL CONTINGENCY LIST and the OBSERVABILITY AREA.

General considerations on mutual knowledge of data

The sensible consideration of surrounding parts of the grid requires an extended and reliable data exchange.

In real time operation solid online exchange of relating topology and measurements is crucial to prevent the depreciation of the quality of state estimation and subsequently of the results of online N-1 calculations.

In the operational planning stage the quality of results depends on the forecast data and especially on the forecasted generation data, which is not yet available for all TSOs.

Due to the aforementioned interdependence of the quality of state estimator results and the provision of external data an adequate backup procedure is recommended in all stages for the cases of missing portions of data from the neighbouring system. For longer lasting disturbances of data provision it could be worth considering online reduction of parts of the surrounding grid to the borders of the own grid.

Considerations on data acquisition when building an External Network for Real-Time State Estimator

National dispatching centers or TSO control centers usually need real-time information about the transmission grid even beyond the national borders or TSO ownership and responsibility borders. To obtain a consistent, reliable set of information on the grid conditions, the control center needs a real-time state estimator which can provide a full AC solution of the modelled network, similar to power flow results.

State estimator treats telemetry or telesignalisation (telemetered quantities, analog measurements and digital status information), from the transmission grid and computes the best estimate of the system state variables (bus voltage magnitudes and angles) and other quantities that can be derived from state variable values (branch flow powers and bus injection powers).

The estimated values are basically analogue values. Digital values can also be estimated by treating them as quantized analogue values (state estimators commonly perform transformer tap estimation, but e.g. switch status estimation is much more difficult and thus hard to find in industrial applications). If the applied algorithm is not capable of estimating digital values, those must be supplied (cannot be unknown) and are treated as fully accurate. For the purpose of this description, only the estimation of analogue quantities will be considered.

State estimator implementations can have different internal algorithms but are common in the objective of finding the best estimate of the system state based on the available measurements. To obtain the best estimate they all try to minimize the total residual which is a certain function of the individual measurement residuals (differences between raw telemetered values and estimated values of measurements). Most widely known approach is the weighted least squares (WLS) estimator, there the total residual to be minimized is the sum of the weighted squares of the individual measurement residual and the weighting factors are associated with the assumed accuracy of the measurements.

If the number of telemetered input quantities is equal or more than the number of state variables to be estimated, the estimation may be feasible — in order to contribute to solvability further conditions are that 1) the input values must be independent in terms of the system of equations of the electrical network (i.e. not be the redundant copies of the same electrical quantity) and 2) the measurements must ”be good” (i.e. not be largely erroneous).

If the state estimation can be performed successfully, the result contains quantities (state variable values and derived quantities) that are observable and may also contain unobservable quantities (if the state estimator is designed to provide a solution for the unobservable network parts, too).

The concept of observability by state estimator can be presented in a simple way:

If an electrical quantity in the modelled network can be estimated (its calculated value can be obtained unambiguously, i.e. there are no multiple possible solutions) based on the available telemetry, then the given quantity is observable. It is important to note that being telemetered does not, by itself, mean being observable and vice versa, being untelemetered does not preclude the possibility of being observable.

When the characteristic quantities of network equipment are observable, the equipment themselves are called observable. E.g. if the power flow on a branch is observable, the branch itself can be termed observable. If voltage magnitude, angle and power injection at a given bus are observable, the bus itself is considered observable. (There can be partial observability in cases of buses, when the voltage components are observable but not the power injection — this bus is then a boundary bus on the edge of the observable area). Contiguous sets of observable buses and branches constitute an observable area.

Since the observability of an electrical quantity in the network model is the result of state estimation, it is very difficult to provide a topological concept for telemetry selection. (Most WLS type state estimator implementations perform a numerical observability analysis at the beginning of the computation process, it is done by Gaussian elimination of the so called gain matrix which contains the parameters of the measurement equations and also the measurement weighting factors. Observability is also affected by measurement errors as most state estimator applications are designed to perform bad data analysis, identification and rejection of erroneous measurements

The OBSERVABILITY AREA has to be fully accurate in terms of topology (all branch statuses and busbar couplers must be telesignalled) and measurement acquisition has to be as complete as possible. It is desirable to have voltage measurements from all buses and active and reactive power measurements from both ends of all branches. It may be acceptable to have some branches that are metered at only one end but then the bus on the unmetered end must have fully metered injection (or be a zero injection bus).

Radial branches can be omitted from the OBSERVABILITY AREA and replaced with telemetered fictitious loads in the connecting grid bus.

It can be advantageous to maintain a so called border or buffer area around the external observability area where the topology is kept actual (branch and bus coupler statuses are telesignalled). It primarily serves the purpose of providing acceptably accurate impedance conditions on both sides of the observability area so that the outage of a branch of the external contingency list can be analysed with good accuracy (limit the effects of topology errors on the observability area). No measurements are needed.

Model termination area is usually created as reduced equivalent of all the remaining external network. It has to provide a terminal impedance which is approximately valid in a wide range of operating conditions, thus facilitate the contingency analysis. No telemetry of any kind is needed.

There exist techniques to somehow improve observability when available telemetry is few. Fictitious measurements (in some contexts called pseudo-measurements) can be introduced for bus voltages, bus injections and (less typically) branch flows. These pseudo-measurements are operator-entered values (or ones that come from historical data processing) that are nominal, typical or expected values for the untelemetered quantities. It is very important that the measurement weight assigned to these pseudo-measurements should be much (e.g. ten times) smaller than that of a real telemetered measurement to tell the state estimator that pseudo-measurements are not expected to be very accurate.

Experience shows that it is difficult to provide good pseudo-measurement values for generation and composite injection (on buses where load and generation co-exist). Bus voltage is an easy candidate for pseudo-measurement, set somewhere near to nominal or typical operational value.

Another way of generating pseudo-measurements can be copying active power (with appropriate sign) from the telemetered end to the untelemetered end of a branch (as long as the loss on the line is relatively low, the new "measurement" will be acceptably accurate).

Step by step implementation of observability area.

Real time Data acquisition

The external representation of network has to be achieved in accordance with the available means of TSOs. The acquisition of data related to network elements situated outside the domestic network can be step by step implemented starting with the external elements located near border that have a significant influence (high influence factor) on the domestic network. The higher is the quality of the risk assessment, the lower will be the value of the influence threshold and consequently the higher will be the magnitude of the size of OBSERVABILITY AREA with external network elements. And then the higher will be the size of real time data to be acquired in the SCADA system.

The size of the of the OBSERVABILITY AREA is part of the TSO's risk assessment that is a compromise between the concern to reduce the risk with the largest network representation and the increase of the cost related to the size to achieve it.

Therefore for TSOs that havn't today a wide representation of external network elements, it is advised to achieve the representation of the OBSERVABILITY AREA step by step.

Security computation

Moreover the computation for security calculation for a wider magnitude of the size of the OBSERVABILITY AREA has an impact on the capacity and performance of tools for the state estimation and to simulate an increased number of contingencies and related costs to install them.

Proposals for algorithms for evaluating the influence of external elements on the responsibility area

In the following two algorithms on the evaluation of the impact of external outages on the responsibility area are described. They offer concrete support in the process of the determination of the OBSERVABILITY AREA, which remains in the end in the responsibility of the single TSO.

Influence factor

The following formula illustrates a method to evaluate the influence of external elements on the responsibility area. By assessing the formula to each external element it is possible to create a ranking of the influence of out-bordering elements in order to identify the external outages that can have a higher impact on the RESPONSIBILITY AREA.

Once the ranking is established, each TSO must select:

- an appropriate CONTINGENCY INFLUENCE THRESHOLD for determining the EXTERNAL CONTINGENCY LIST. If the INFLUENCE FACTOR of an external element is higher than the threshold, this element should be considered as part of the EXTERNAL CONTINGENCY LIST.
- an appropriate OBSERVABILITY INFLUENCE THRESHOLD for determining the EXTERNAL OBSERVABILITY LIST. If the INFLUENCE FACTOR of an external element is higher than the threshold, this element should be considered as part of the EXTERNAL OBSERVABILITY LIST.

Abovementioned threshold values have to be established taking into account that the INFLUENCE FACTOR calculated represents the maximum expected load increase in an internal element of its network as a consequence of the external element outage.

Permanently Admissible Transmission Loading (PATL) is the loading in Amps, MVA or MW that can be accepted by a branch for an unlimited duration.

The INFLUENCE FACTOR of an external branch *r* on the RESPONSIBILITY AREA could be calculated according to the following formula:

$$In_r = \max_{\forall t \forall i (i \neq t)} \left(\frac{P^t_{n-1} - P^t_n}{PATL^t} \cdot \frac{PATL^r}{P^r} \cdot 100 \right)$$

In_r : Influence factor of an external branch *r* on a branch *t* of the responsibility area

t: Branch of the responsibility area where the active power difference is observed

i: Branch of the responsibility area (different from branch *t*) considered disconnected from the network when assessing the formula $\frac{P^t_{n-1} - P^t_n}{PATL^t} \cdot \frac{PATL^r}{P^r} \cdot 100$

P^t_{n-1}: Active power through the branch *t* with the external branch *r* and the branch *i* disconnected from the network.

P^t_n : Active power through the branch *t* with the external branch *r* connected to the network and the branch *i* disconnected from the network.

P^r : Active power through the external network *r*, when connected to the network, considering the branch *i* disconnected from the network.

$PATL^t$: PERMANENTLY ADMISSIBLE TRANSMISSION LOADING (PATL) of the branch *t* (in MVA)

$PATL^r$: PERMANENTLY ADMISSIBLE TRANSMISSION LOADING (PATL) of the external branch *r* (in MVA).

The formula $\frac{P^t_{n-1} - P^t_n}{PATL^t} \cdot \frac{PATL^r}{P^r} \cdot 100$ must be applied, for each external branch *r*, assessing its influence on every branch *t* of the RESPONSIBILITY AREA, and considering any possible outage (branch *i*) within the RESPONSIBILITY AREA[3]. The INFLUENCE FACTOR of an external branch *r* is the maximum value of the previous calculations. Therefore, assuming a RESPONSIBILITY AREA with K

3 In order to consider different possible operational situations.

branches, for each external branch *r*, the formula $\frac{P_{n-1}^t - P_n^t}{PATL^t} \cdot \frac{PATL^r}{P^r} \cdot 100$ must be evaluated K*(K-1) times in order to get the influence factor In_r of that external branch *r*.

Influence factor linked with Influence Threshold

The elements to be put in the observability area are determined by comparing their influencing factor with the influence threshold. The influence factor (in percentage) of an element *r* on the an element *t* can be calculated according to the following formula:

$$F_r^t = \left(\frac{P_{n-1}^t - P_n^t}{P^r} \cdot *100 \right)$$

F_r^t : Influence factor of an element *r* on an element *t*

P_{n-1}^t: Active power through the element *t* with the element r disconnected from the network.

P_n^t : Active power through the element *t* with the element *r* connected to the network.

P^r : Active power through the element *r*, when connected to the network.

The influence threshold can be calculated according to this formula :

$$T = \left(\frac{I_i^{N-1} - \alpha_i I_i^N}{\alpha_e I_e^N} \right) *100$$

T : Influence Threshold

I_i^N : PATL of the internal element *I* in the N case (To be clarified)

I_i^{N-1}: PATL of the internal element *I* in the contingency case.

I_e^N : PATL of the external element *e* in the N case.

α_i : load factor (i.e : I/Imax) of the internal element i admissible in operational condition.

α_e : load factor (i.e : I/Imax) of the external element e admissible in operational condition (if no info : 1 should be taken).

The calculation of the influence threshold can be performed for each element. In order to decrease the number of calculations, one suggests to define a unique minimum influence threshold by taking into account the worst case i.e. the lowest transmission capacity for the internal elements (N and N-1 case) and the biggest transmission capacity for the external elements.

An external element e should be taken into account as part of the observability area when the condition I_e^i ≥ T is fulfilled. Such calculations should be made using different time frames.

4. - DEFINITION OF OPERATING LIMITS

Background

The aim of defining operating limits is firstly to protect the people at the vicinity of the materials (near conductors) and to protect the materials that are designed for operation below their technical limits.

The structure of the networks is also designed following a country policy.

Therefore, the country approach to operate the materials is left to subsidiary in accordance with grid codes. And the way to operate the material and consequently the network can result from different philosophy.

This chapter deals with three types of parameters :

- flows on lines, cables or transformers,
- voltage on nodes of a network,
- voltage phase angle differences.

Flows on lines, cables or transformers

An overhead line is designed taking into account a maximal permissible temperature of its conductors. Even if the conductors reach this maximal permissible temperature, the isolation distance must be respected as to ensure the safety of any people or any infrastructure all around the line.

In operation, the temperature of the conductors depends on several factors but the most dominating one is the intensity through the line in Amps. The temperature of the conductors depends also on the weather conditions: air temperature, wind (direction and speed), precipitations (snow, ice storms) and solar radiation. The variability of such weather conditions can induce some TSOs to consider two or three seasons (winter, summer and sometimes intermediate season). Another solution consists in choosing the lowest value (summer) with permissible overload during colder weather conditions. The average weather conditions for each season come from statistic analysis based on the past years data.

The thermal inertia of the conductors has also to be taken into account. For a given intensity, the final temperature of the conductor is not reached immediately. The higher the intensity, the faster the maximum permissible temperature of the conductors will be reached.

The cables and the transformers are also designed for a maximum permissible temperature of their conductors, but a higher thermal inertia has to be considered.

Ancillary equipment associated with a transmission line or a transformer, such as current and voltage transformers for measurement, disconnectors, power circuit breakers, high frequency chokes, busbars capacities, might be, in some cases, the limit of the transmission capacity (bottleneck) for lines/cables/transformers.

Taking into account all these phenomena, TSOs calculate for each line, cable or transformer the **Permanently Admissible Transmission Loading (PATL)**: this is the loading in Amps, MVA or MW that can be accepted by a branch for an unlimited duration.

In N situation, every network element is due to be operated below its Permanently Admissible Transmission Loading (no permanent overload is allowed).

In N-1 or N-k situation, an overload regime starts beyond the Permanently Admissible Transmission Loading. This overload regime can be managed in different ways :

- no overload is allowed, with a PATL not to be over-passed,

- a **Temporarily Admissible Transmission Loading (TATL)** that is an overload corresponding to a fixed percentage of the PATL for a given time is allowed (for example, 115% of the PATL can be accepted during 15 minutes); these overload conditions are applied for the whole network but can be different from a voltage level to another one,
- several **specific couples (TATL, admissible duration)** are calculated for each line taking into account its particular configuration and conditions of functioning (for example, for a given line, it can be defined one TATL acceptable during 20 minutes and another one acceptable during 10 minutes).

In case of applying an overload regime, considering the loss of a network element (N-1 state), overloads on impacted network elements are admitted only if remedial actions are available in the allowed time as to get back any network elements below their respective PATL. If the allowed time corresponding to a given TATL is violated, the branch is due to be considered as tripped in the network calculations. This situation can be admitted only if there is no uncontrolled evolution for the overall system (cascading tripping, voltage collapse, loss of synchronism); if not, preventive remedial actions are required.

In case of a situation beyond the TATL, an ultimate intensity is defined as the threshold the line will immediately trip without any possible remedial actions, determined to serve for selective fault clearance. It is called the **Tripping Current without delay (TC)**. This value can also be applied in consideration of the potential bottlenecks of some substation equipments.

All these values are described on the figures 6 to 8 below mentioned. The figures 6 to 8 represent two common approaches on the application of the limits described above. They do not have an exhaustive pretension. Different versions can exist depending on individual conditions.

For some particular network elements like cables or transformers, for which thermal inertia is much higher than the one of overhead lines, it is admitted to exceed the PATL in the N state for a known in advance temporary duration (for example during a period of one hour before and after the peak of consumption). In any case, the overload conditions (depth and duration) have to be respected and if not, preventive remedial actions are required.

Management of the PATL and the overload conditions

The respect of the PATL and, if implemented, the respect of the overload conditions (TATL and duration) can be assumed:

- <u>by the dispatcher</u> who can be supported for that by his SCADA; in real time, in case of violation of the PATL or TATL respectively, no device will order the tripping of the line; in that case, it’s up to the decision of the dispatcher to open the network element.
- <u>by overload protections</u> in which several couples (TATL; admissible duration) can be implemented; if the loading has not come back under a given TATL after its allowed duration, this protection will order immediately and automatically the tripping of the network element without any possible action of the dispatcher as to stop this process.

The Tripping Current without delay (TC) can be monitored by a distance protection or by an overload protection, but in any case, the tripping of the line will be ordered immediately without any possible remedial actions, and is effective at the end of the cycle of the protection device (less than one second in case of a distance protection, less than one minute in case of an overload protection).

Information sharing

The information on values of PATL, TATL and TC of their tie-lines and of the elements of the observability lists must be shared among neighbouring TSOs (mutual information procedure must be implemented).

Seasonal and weather conditions approaches

The operating limits of each element can change depending on the season or on the weather conditions. TSOs, which use overload protection devices change the settings of these devices accordingly.

For some TSOs, the operating limits and protection settings are changed for the winter or summer periods. For some other ones, some intermediate regimes exist. For some others, there exists a system to follow-up the real time weather conditions (temperature, wind speed and direction, sunshine), which can lead to adapt the operating limits of the network elements.

For some TSO, only distance protections exist as the protection devices are not regarded to serve as an overload protection.

Security margin

A margin from the TC is applied as to take into account the uncertainties on measurements, on the set-up of the protection values and the inaccuracies of security calculations and to some extent the transient effects of topology changes,. This margin is determined by each TSO taking into account its own experience. It is applied at least in day ahead and real time operation but it can also be applied in the planning stage.

Applying this margin determines an operating threshold (TC – margin) for the instantaneous tripping of each network element which can be taken into account in the network calculations called the Instantaneous Tripping Threshold (= T_3 in the figures 6 to 8 below).

Alarms generated by N-1 security calculations

In real time operation, a warning is given to the dispatcher by the SCADA if any flow on a line, a cable or a transformer is higher than X% of the PATL for the given season. The warning values delivered by the SCADA can be different from one TSO to another, as based on different policies. This threshold can be adapted in real time by the dispatchers, depending on the design of the single SCADA system. The warning value (X%) can vary from 50% to 100% and also beyond.

In N-1 security analysis, following the automatic calculations, a list of constraints is generated corresponding to those elements exceeding the PATL or exceeding an overload threshold. It leads the dispatcher to:

- acknowledge the value of loading resulting from the contingency simulation and for TSO not applying an overload regime to conduct preventive remedial actions in case of exceeding the PATL of a network element, (refer to figure 6 below),
- verify the availability of remedies and the compatibility of their implementation duration for TSO applying an overload regime; if not, the network element has to be considered as tripped which can lead the dispatcher to launch preventive remedial actions. (refer to figures 7 and 8 below).

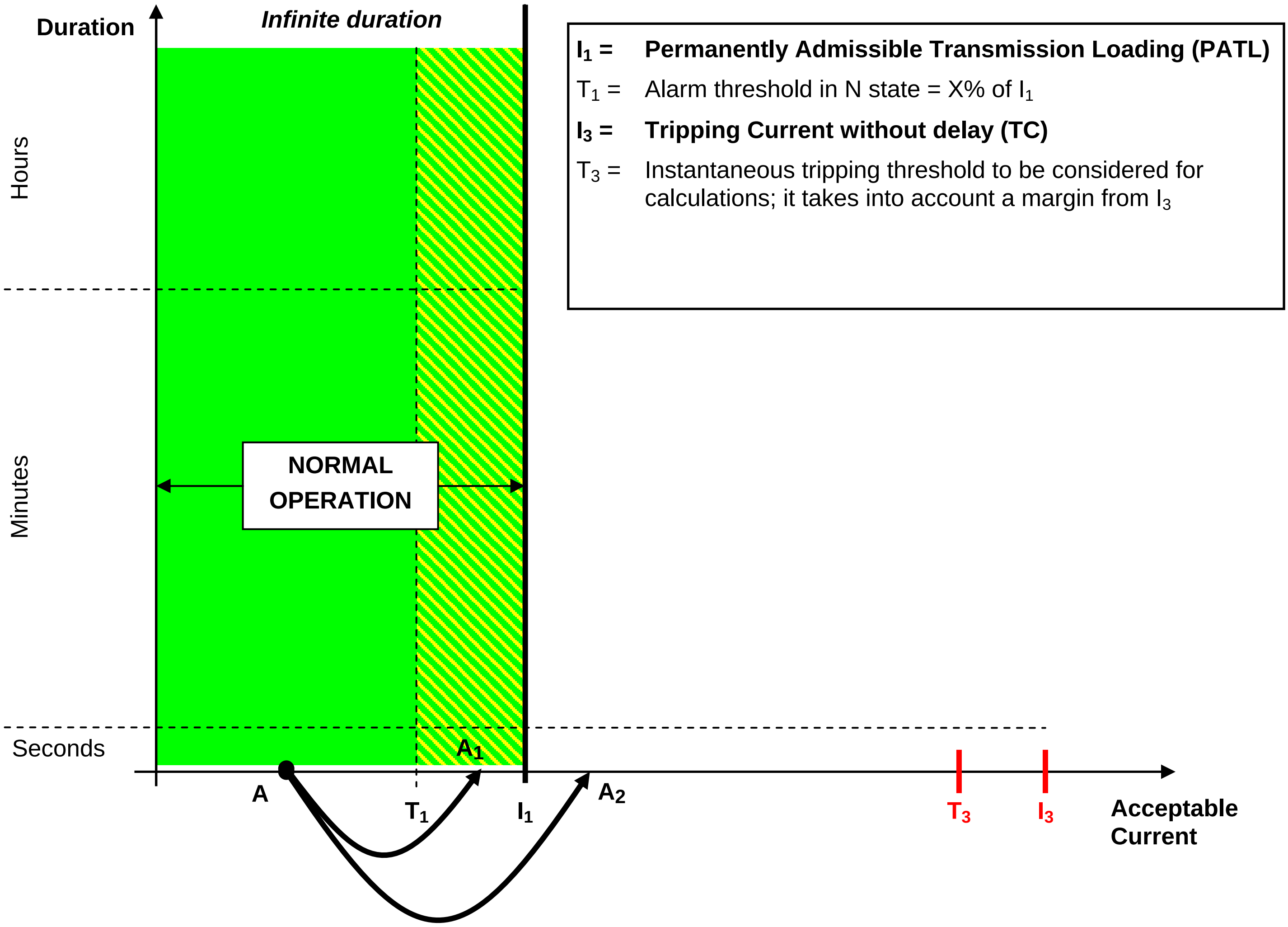


Figure 9: Acceptable loading on a line depending on duration

First case : No overload regime is applied

Starting from A point on figure 6 above: the studied tripping can lead to two cases:

- for the case A_1, N-1 is OK because the loading on the impacted network element is below its PATL (I_1),
- for the case A_2, N-1 is Not OK because the loading on the impacted network element is beyond its PATL (I_1) ; in that case, preventive remedial actions are required as to ensure a loading below I_1 after the studied tripping.

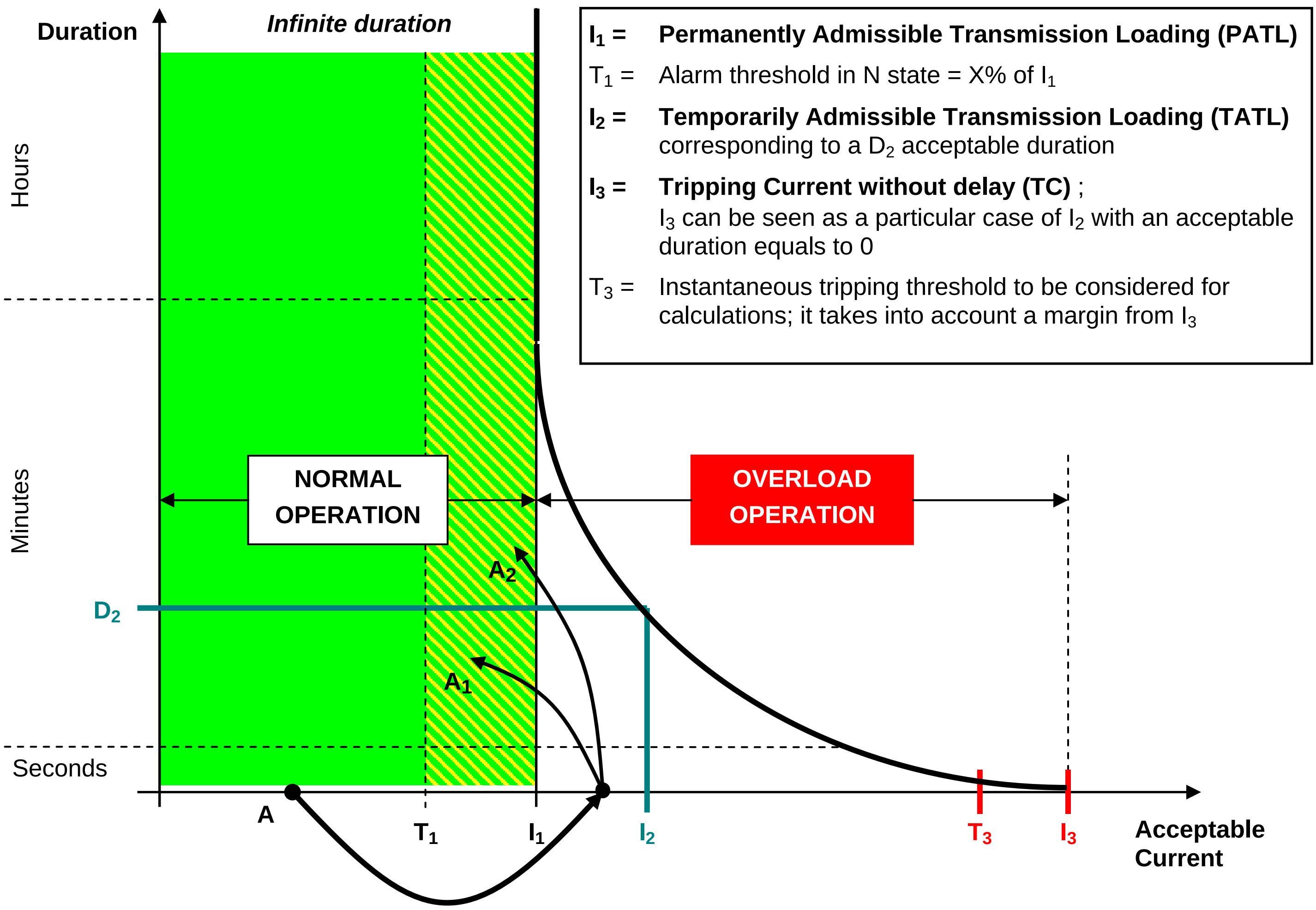


Figure 10: <u>Acceptable loading on a line depending on duration</u>

<u>Second case :</u> An overload regime is applied with only one couple (TATL; admissible duration)

<u>Starting from A point on figure 7 above:</u> the studied tripping leads to an overload on an impacted network element but below its TATL (I_2); TSO has to verify that there are enough remedial actions to bring back the loading on the impacted network element below its PATL (I_1) in a time less than the respective admissible duration D_2:

- for the case A_1, N-1 is OK,
- for the case A_2, N-1 is Not OK because I_1 can not be reached before D_2; in that case, the induced tripping of the impacted network element has to be considered in studies and if this tripping leads to an uncontrolled evolution of the system, preventive remedial actions are required.

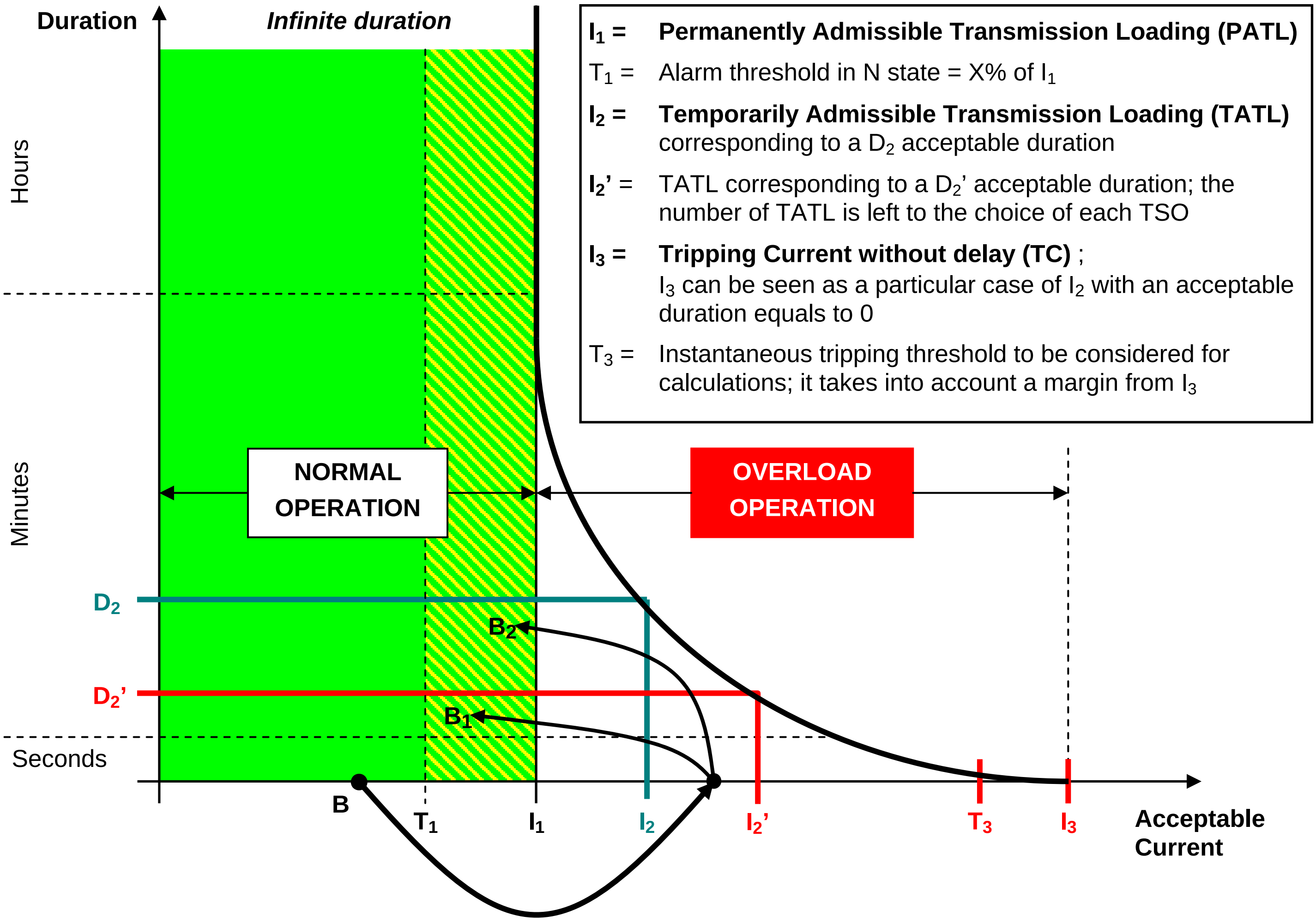


Figure 11: <u>Acceptable loading on a line depending on duration</u>

<u>Third case :</u> **An overload regime is applied with several couples (TATL; duration)**

<u>Starting from B point on figure 8 above:</u> the studied tripping leads to an overload on an impacted network element above its TATL (I_2):

- if the TSO applies only one TATL value (I_2), the induced tripping of that network element has to be considered in N-1 calculations and if this tripping leads to an uncontrolled evolution of the system, preventive remedial actions are required;
- if the TSO applies two TATL values (I_2 and I_2'), it has to verify that there are enough remedial actions to bring back the loading first below I_2 in a time less than D_2' and second below I_1 in a time less than D_2 minus the time already used above $\mathbf{I_1}$:
  - for the case B_1, N-1 is OK,
  - for the case B_2, N-1 is Not OK because I_2 can not be reached before D_2'; in that case, the induced tripping of the impacted network element has to be considered in studies and if this tripping leads to an uncontrolled evolution of the system, preventive remedial actions are required.

Voltage in nodes of a network

The voltage must be maintained throughout the network within a range of values in order to:

- be compatible with the sizing of the equipment,
- maintain the supply voltage of customers within the contractual ranges,
- guarantee the system reliability and avoid the occurrence of voltage collapse,
- maintain static stability.

Sizing of the equipment

Voltage too high can lead to accelerated ageing or the destruction of the equipment. Generally, the upper limit is around 420 kV for the 380-400 kV network and around 245 kV for the 220-225 kV network. Exceeding can be acceptable but for a limited time duration according to TSO's internal rules[4].

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

Contractual ranges for customers

For customers and distributors, each supply contract defines the declared supply voltage value and the accepted variation range around this value or thresholds. These two terms, depending on the sizing of customers equipment connected to the network, must be respected at all times.

Voltage collapse

For each operational situation there is a maximum active power that can be transmitted through the network. This point is called the critical point and represents the point where the system collapses. As long as the load increases, the power transmitted to supply the load also increases meanwhile the voltage profile of the network decreases in inductive network. Close to the critical point, a small increase of the demand/load implies a great decrease in the voltage level of the network. It can be summarized in the curve hereafter.

Margins from the critical voltage

The critical value of the voltage of each node of the grid is a function of the characteristics of the grid and of the load (inductive or capacitive) and of the location of the reactive compensation means.

The margins to keep voltage secure depends on reserves of reactive power generated either by the network itself or by reactive power available at generating units or by bank capacitors. The management of this margin is not easy for any network. The danger comes from limiters of reactive power of generation units.

For radial network, it is easier to calculate the reserve of reactive power that will be efficient to maintain the voltage values than for meshed network.

---

4 For example, it can be admitted for the voltage to be between 420 kV and 424 kV less than 20 minutes, or between 424 kV and 428 kV less than 5 minutes. The respect of high voltage level on equipment can lead TSOs to switch-off a line with a very low load (this functioning regime provides reactive power that contributes to increase the voltage level) especially during off-peak hours

At any time, TSOs must guarantee that in N and N-1 situations the voltage level is not near the critical voltage. This rule leads TSOs to determine acceptable voltage levels for the N situations and potentially different ones corresponding to N-1 situations.

These voltage levels have to include margins from the critical voltage. They can be the same for all the nodes of the network. But, sometimes, it can be necessary to calculate specific voltage levels for particular nodes.

VOLTAGE BEHAVIOUR OF THE POWER SYSTEM

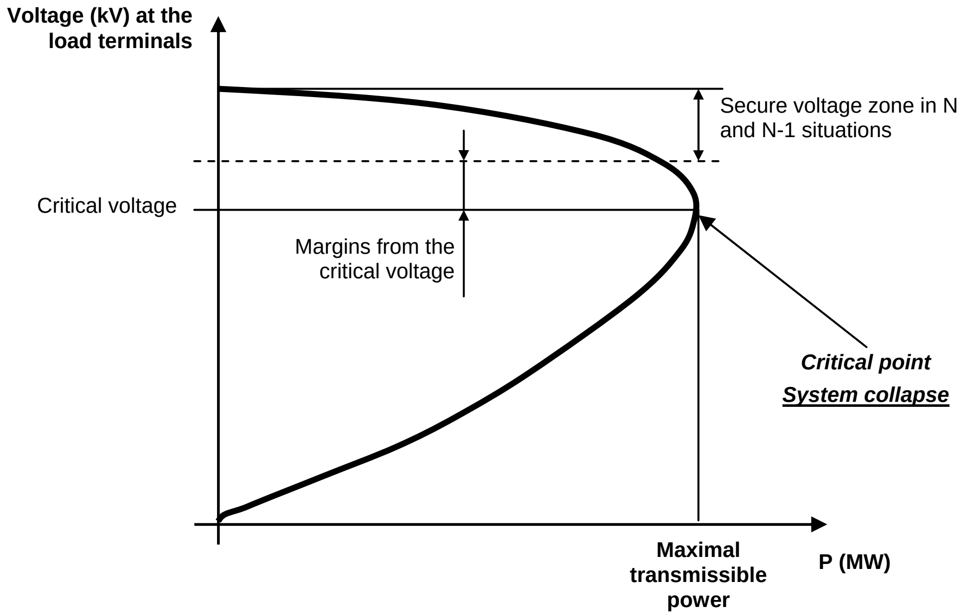


Figure 12: Voltage behaviour of a power system

VOLTAGE LIMITS

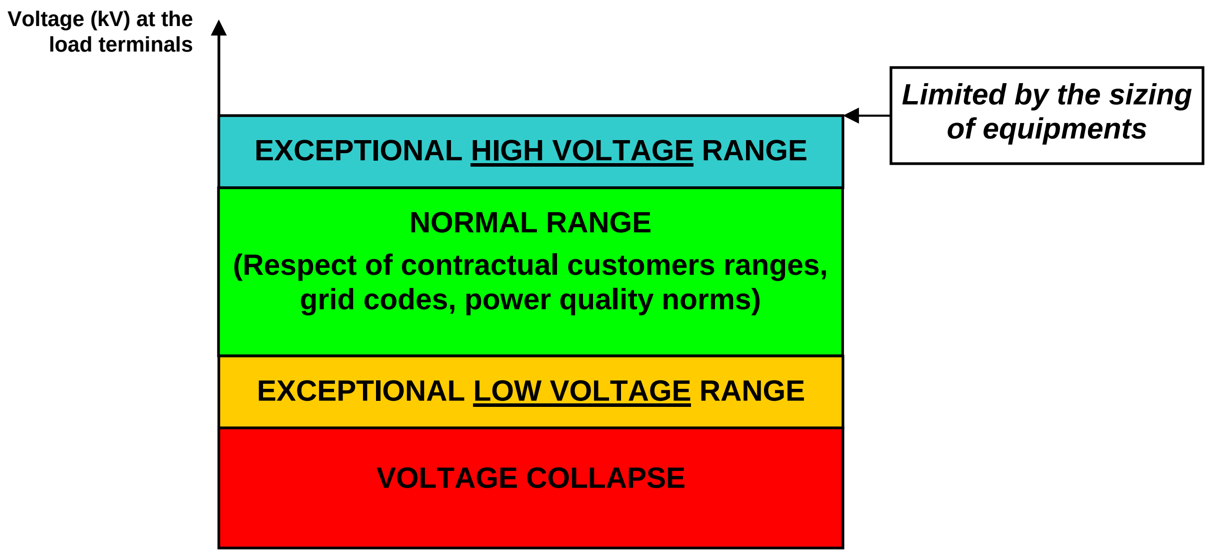


Figure 13: Principle of voltage limits

Voltage Phase Angles Differences

Following the opening or the outage of tie-lines a manual reclosure may be refused by Parallel Switching Devices (PSDs) in case of voltage phase angle difference exceeding the preset threshold of the device.

The setting of the threshold depends on operational conditions in this respective area of the grid. As the values are often chosen around 30^o they may also be significantly lower if large generation units are near to the tie-line. The stability of such generators may be jeopardized or at least heavy oscillations can be started by switching operations performed with high voltage phase angle differences. The stability can be slightly enhanced by avoidance of under-excitation of the generator.

Reclosure may be forced with by-passing the PSDas a measure of last resort mainly managed by a local operator in the substation. It is of utmost importance to perform if possible a dynamic simulation considering that a state estimator calculations is not sufficient to determine secure limits after reclosure. Reclosure can also be possible even with unusual high angles of $40\ldots50^o$, but it is needed to reduce the angle prior to switching by means of re-dispatch or by changing taps of PSTs.

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

In every case reclosure actions have to be coordinated and agreed with every possibly affected neighbouring TSO.

5. - Remedial actions and ASAP (As Soon As Possible) for grid constraints

Introduction

The goal of remedial actions is to fully respect the N-1 principle taking into account inter-TSOs coordination. After a normal or exceptional type of contingency, the situation should be without constraints after implementation of remedial actions when needed. In any cases, cascading effects across borders must be prevented by remedial actions. In this case remedial actions make sure that the N-1 principle "**no cascading with impact outside my borders**"[5]is respected at all time.

Remedial actions

Remedial actions are defined for the two reference grid constraints related to

- Power flows,
- Voltage.

Any network event or contingency related to one of these two reference issues can impact the other one. The remedial actions decided by a TSO for each event can differ from one occurrence to another depending on the power system conditions of operation.

Preventive (before occurrence of the contingency) and curative (after occurrence) remedial actions are due to be previously prepared in operational planning stage and to be duly applied in real time.

These remedial actions (preventive/curative) have to be previously assessed by numerical simulations in order to evaluate the influence of those measures on the constraints and also to prevent negative effects to neighbouring TSOs.

In all cases when a contingency (or a remedial action) can affect neighbouring TSOs, after a due common information exchange, involved TSOs check together the efficiency and the consequences of the remedial actions by an additional N-1 computation. Such checking is primarily achieved in operational planning.

- TSOs are committed to prepare in anticipation remedial action for the Day D, in coordination with neighbors.
- The remedial actions applied by a TSO shall be checked by numerical simulations in order to prevent obviously counter-effects to neighbouring networks.
- The remedial actions have to be agreed by them in advance if possible by TSO to TSO procedures or by regional inter-TSOs procedures.

---

5 The principle to be used is to prevent cascading effects of a contingency: Each TSO simulates the possible cascading effects in order to check if the collapse could propagate at least till the boundary, given the neighbour is alone the best place to simulate the progression of this cascading effect within its respective grid. In this case the originated TSO informs the possibly affected neighbour in order it checks the situation within its respective grid and provides its neighbours with all needed elements for simulations.

At the moment the DACF procedure provides the data for the simulations but is not set up to offer a standardized tool to study possible cascading effects especially on neighbours. Such approach exists at present in day ahead for example with DACF files.

To relieve constraints applying remedial actions, the escalation principle is as follows:

The TSO implements remedies with the minimum delay. Whatever in the operational planning stage or in real time, the regional coordination eases and enhances the search of (possible, but not optimized) coordinated solutions in case of a call for help. In any case it is encouraged to contact neighbours ASAP even at the beginning of the process to search for remedies.

- Firstly the impacted TSO who is monitoring a constraint violation, checks the implementation of internal remedial actions by itself.
- If the internal remedial actions are not efficient[6], remedial actions are defined by a co-ordination between neighbours in order to set-up the most appropriate remedial actions.
- These additional actions are due to be implemented in the originated control area (where the contingency occurs) or in the other impacted control area(s).
- The regional coordination to prepare common remedial actions can involve other less impacted control areas.
- At this stage specific analysis for costly measures taken by one or several TSO to implement remedial actions is to be dealt with in the framework of bi/multilateral TSO to TSO procedures, e.g. with respect to Policy 5

ASAP and Compatible delay with constraint to relieve

The notion of ASAP is related to the delay of remedial actions implementation to come back to a N-1 secure situation after the occurrence of a first contingency to cope with the following (second, etc.) contingency to come. During ASAP, the system is put at risk.

1.a. – **First contingency always covered by remedies**. For any situation of the system at any time, the new N-1 principle requires that after a first contingency, TSOs are always required to have ready and checked remedial actions to be launched in advance or without delay and very rapidly efficient after the occurrence of a contingency. The first contingency is covered at least by mandatory curative remedial actions efficient in a very short while of some minutes (e.g. 15 min/20 min) to keep the system secure [new N (=Ñ) is OK, but new Ñ -1 can be not OK] .

1.b. – Second contingency covered by remedies ASAP.

Once the contingency occurs, that means once a N-1 occurs, and the TSO has applied already prepared in advance remedies (refer to 1.a), the impacted TSO being then in a secure situation Ñ (Ñ =N-1 + applied remedies) shall launch security calculation to detect the risk and prepare new remedies. The remedies are related to changes of topology, of redispatching, and of counter-trading to be prepared by a TSO either by its own or with neighbours. The TSO implements remedies with the minimum delay (ASAP). The regional coordination eases and enhances the search of (possible, but not optimized) coordinated solutions in case of a call for help. In any case it is encouraged to contact neighbours in the shortest delay even at the beginning of the process to search for remedies.

After occurrence of the first contingency and the performance of the already prepared remedial actions, if the remedies for a Ñ-1 contingency to come are available and efficient in a short while, the system is OK.

When remedies are not sufficient, the TSO informs neighbours about the delay of remedies and calls for help to avoid or reduce the delay. That means that new remedies to be launched cannot be either available or efficient in a short while, putting the system at risk, like e.g. (i) in case of starting a cold power plant that will be connected in a while of eight

6 “Efficient” means that remedial action are prepared with respect to the compromise between their effectiveness and their costs and are rarely extremely expensive

hours, or (ii) in case that a return to operation of a scheduled outage within a delay of two hours; (iii) in case of damage due to storm, the impacted TSO could need days in order to fully comply with the N-1 principle. In these three cases the system is at risk in the while of full effectiveness of remedies.

The study of new remedies (to come back to a secure situation if occurrence of a new N-1) cannot last too long because in the meanwhile the system can be jeopardized after the contingency if no convenient remedies have been identified. Therefore in a short while the TSO has to coordinate future remedial actions with neighbours.

The **delay of ASAP cannot be estimated** because it depends on the available remaining facilities of the power system (a part of them having been used to face the constraints appeared after the first contingency) and on the risks in terms of cascading effects.

To some extent, the longer the time frame between the first and the second contingency, the better the availability of facilities to relieve congestion and the time to prepare remedial actions to recover a secure operation, but the risk of collapse lasts in the while.

During such situation, the TSO which is in “Alert”, provides the necessary information to neighbours and searches convenient remedial actions also with them

SHORT ASAP

If the situation can be secured after a shorter delay than the implementation of a costly remedial action (coupling of a power plant that can last 8 hours), the TSOs are allowed to be in ASAP. E.g. case of a scheduled outage with return to operation within 2 hours compared with the need of the start of a power unit lasting eight hours: the TSO doesn’t launch the order to start the unit and takes the risk. He should inform its neighbours.

LONG ASAP

After a serious contingency, like the destruction of a pylon, the remedial actions cannot always be ensured day ahead for the Day D and beyond to cover the occurrence of a new outage (Ñ-1).

In this case, the TSO shall find solutions with neighbours to secure the system and be ready for the occurrence of emergency solutions.

In such an insecure situation ASAP lasts a long while, although some co-ordinated remedies have been activated.

RISK MANAGEMENT

ASAP – AS SOON AS POSSIBLE AND REMEDIAL ACTIONS

Figure 14:

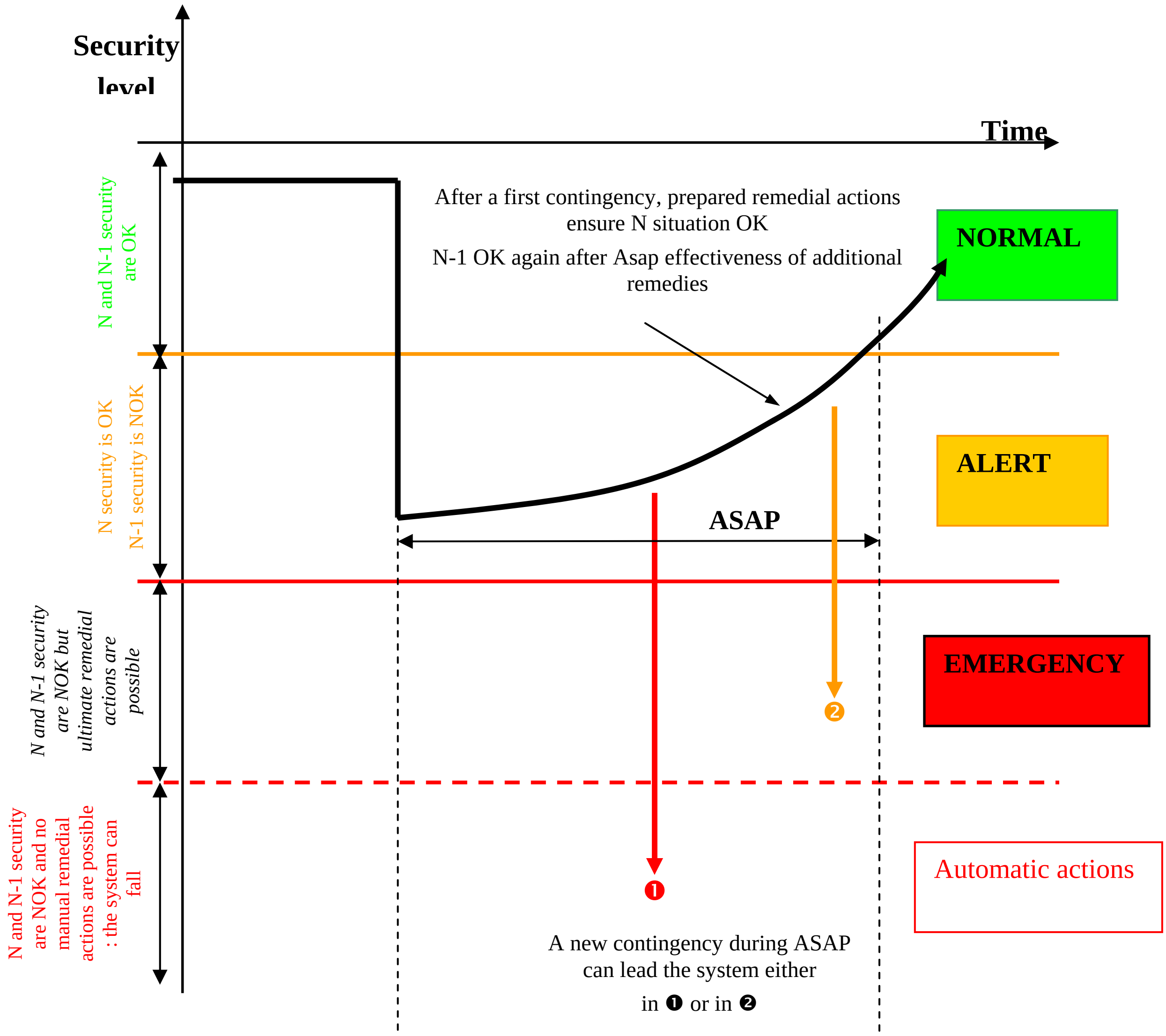


Figure 15: Notion of “asap” in relation to power system levels

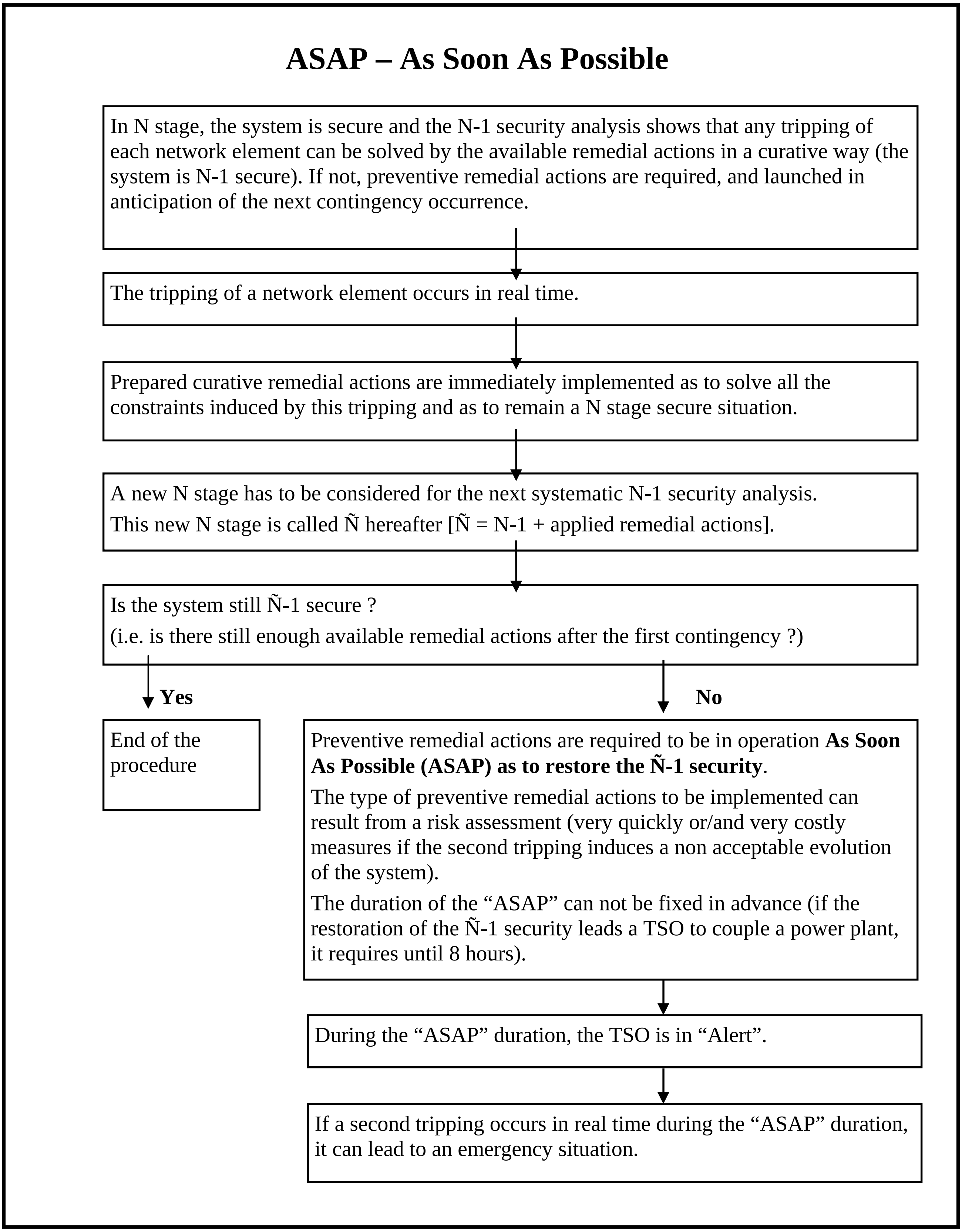


Figure 16: Process for restoration of N-1-security after an incident

Degree of Acceptance of "no possible remedial solutions" by a TSO

In line with the above-mentioned situation, in case of preparing a Ñ-1 contingency (the second one), a TSO can face impossibility to cover the risk, having done its “best efforts” (no topology efficient, no generation redispatching available) in a first stage. That can be the case of (i) a small system with high loop flows or (ii) problems of wind farms management, etc. so that TSO cannot relieve congestions by its own and puts the regional system at risk.

That highlights the **importance of regional coordination and common approach:**

- To do the same simulations of risk and same simulations for remedies efficiency.
- To increase the chance to find remedies.
- To optimize solutions. And then to anticipate and solve situations at risk.
- To prepare procedures or agreements for coordinated remedies.
- To share or clear cost of remedies applied by neighbours (redispatching, counter-trading, emergency reserve).

- **Consideration to manual load shedding as the ultimate remedy**. In the case a TSO puts the system at risk, the ultimate solutions to be explored consist in the impact of the market (stop of wind-farms, capacity curtailment) that should be mandatory. If all the remedial actions are not sufficient (after escalation of cross-border topology, cross-border redispatching, counter-trading, market curtailment), the emergency procedures (Cf. Policy 5) are applied, including manual load shedding.

  Do we consider manual load shedding as mandatory to be applied by the TSO in difficulty? In this case, the system can be operated at risk (ASAP situation and/or risk of uncontrollable cascading effects) by a TSO only under the condition of this mandatory manual load shedding always ready (press-button action with efficiency in a very short while of a few minutes that means tools to customizily “telecontrol” load shedding - what might be realizable only in the long run for some TSOs).

Impacting effect			
	TSO A	**TSO B**	**TSOs in Region**
Simulations based on contingency list (external and internal network elements) **Remedial actions and domestic operational decisions**	Check inside Risks at home (from outside contingencies) Risk to neighbour(s) (cascading risk from inside contingencies or external impact of domestic decisions/actions)	Informed by TSO A of risks Bilateral coordination of remedies: Rapid or ASAP If ASAP, ALERT	All TSOs involved or impacted in the region All informed by TSO A of risks Multilateral coordination of remedies[7]

Figure 17: Inter-TSO coordination from bilateral to multilateral/regional

7 With a regional Coordination for risk analysis, where that (will) exist, it could be done a detection of risks in a multilateral way.

Remedial actions summary table

Remedial actions are classified by TSOs under their individual approach in accordance with their grid codes. TSOs consider in all cases

- an escalation of measures - post event/curative and preventive.
- non cost and cost measures

Some of the following measures are not available due to national legal framework.

(Non exhaustive list)

Power Flow Constraints

- Topology changes (network reconfiguration).
- Use of phase shifter transformers.
- Cancellation of maintenance (grid elements urgently backed to operational service).
- Changes in the pattern of reactive power flow:
  - within own grid,
  - with the support of neighbouring TSOs.
- Automatic unit tripping triggered by line outage.
- Deployment of tertiary reserves.
- Contracted generation re-dispatch within the TSO’s own control area.
- Cross-border redispatching with neighbouring TSOs.
- Counter-trading with neighbouring control areas.
- Intervention in scheduling:
  - freezing of scheduled exchanges,
  - schedule of exchange reduction.
- Reduction of interconnection capacities.
- Start-up of tertiary reserve (hydro, pumping, rapid thermal units and others).
- Pump tripping.
- Manual load shedding of interruptible loads (customers).
- Automatic shedding of interruptible customers triggered by line outages.
- Manual load shedding of domestic loads.
- Automatic load shedding of loads.

Voltage Constraints

- Requesting maximum or minimum values of generation for active and reactive power (P and Q).
  - Reduction of active power in favor of additional reactive power output.
- Manual tap changing of 380/220-kV-transformers.
- Adjusting of power flows.
- Switching on/off shunt reactors or capacitors.
- Preventive start of units with provision of additional reactive power.
- Line opening in case of high voltage conditions (off-peak periods).
- Stop of voltage and reactive power optimization.
- Stop of maintenance, switching-on of all elements previously in maintenance.
- Limitation of intraday trade (influence on transits).
- Blocking of OLTC (On Load Tap Changers) of transformers.
- Changes of voltage regulator set points on transformers at distribution level.

- Manual load shedding of interruptible loads (customers).
- Manual load shedding of domestic loads.
- Automatic load shedding.

Remedial actions – summary table in appendix

The following table “remedial actions – best practices” in appendix presents a non exhaustive list of remedial actions to be applied on the power system. It contains an indication about escalation of the remedies from operational planning to real time and from normal situation to dangerous situation, from non costly to costly actions, from seconds to hours of delay of reaching full effectiveness of the remedies:

- escalation of remedial actions,
- delay of full effectiveness of remedies,
- from operational planning to real time,
- from normal situation to emergency,
- from topology changes to load shedding.

REMEDIAL ACTIONS

BEST PRACTICES

actions	Time constant	cost	P/C	A/M	Y-1	W-1	D-1	Normal	ALARM	Emergency
predefined automaton action (generation tripping or load redistribution/cutting in case of outage)	a few milliseconds	no cost	C	A	-	-	-	x	x	x
topology modification via breakers	a few minutes	no cost	P/C	M	x	x	x	x	x	x
topology modification via switchers	Minutes or Hours : depending on the avaibility of grid operator	no cost	P	M	x	x	x	x	x	-
transformer tap position modification	a few minutes	no cost	P/C	M	x	x	x	x	x	x
capacitor or reactor switching on/off	a few minutes	no cost	P/C	M	x	x	x	x	x	x
PST tap position modification	a few minutes	no cost	P/C	M	x	x	x	x	x	x
Load redistribution	a few minutes	no cost	P/C	M	x	x	x	x	x	x
Mvar production modification on generation units	a few minutes	low cost	P/C	M	x	x	x	x	x	x
Pump tripping/starting	a few minutes	low cost	P/C	M	x	x	x	x	x	x
internal I/D bids on generation units (internal redispatching)	a few minutes	low cost	P/C	M	-	x	x	x	x	x
Start/Stop generation unit	Minutes or Hours : depending on the type of unit	low cost	P/C	M	x	x	x	x	x	x
International I/D bids on generation units (international redispatching)	a few minutes	low cost	P/C	M	-	-	x	x	x	x
outage planning modification		costly	P	M	x	x	x	x	-	-
outage restitution	Many hours : depending on the restitution delay	costly	P/C	M	-	-	-	x	x	x
limitation of exchange capacity		costly	P	M	x	x	x	x	x	x
contractual manual load shedding	a few minutes	costly	P/C	M	-	-	-	x	x	x
cross-border exchange modification (curtailment)		costly	P/C	M	x	x	x	x	x	x

Non contractual manual load shedding	a few minutes	costly	P/C	M	-	-	-	-	x	x
MV voltage settings down (5%)	a few minutes	emergency	C	M	-	-	-	-	x	x
(Automatic) disconnection of border lines	a few seconds	emergency	C	A/M	-	-	-	-	x	x
blocking of OLTC	a few minutes	emergency	C	A	-	-	-	-	x	x
Automatic load shedding	a few minutes	emergency	C	A	-	-	-	-	-	x

A/M	Automatic/manual
P/C	Preventive or curative action
-	not applicable

The curative actions can be applied only if the time needed to implement them is less than this time needed to releave the violation in a safety way for the grid (notion of temporary maximal limit)

.

This time could be higher only if it was confirmed that the violation can be safety supported by the grid for a longer period (notion of temporary maximal limit)

Figure 18: List of remedial actions

6. Power System Stability

The classification of Power System Stability is convenient in identifying causes of instability, applying suitable analysis tools, and developing corrective measures. In any given situation, however, any one form of instability may not occur in its pure form. This is particularly true in highly stressed systems and for cascading events; as systems fail one form of instability may ultimately lead to another form. However, distinguishing between different forms is important for understanding the underlying causes of the problem in order to develop appropriate design and operating procedures.

The classification proposed here is based on the following considerations:

§ The physical nature of the resulting mode of instability as indicated by the main system variable in which instability can be observed : Rotor angle, Frequency or Voltage Instability;

§ The size of the disturbance considered, which influences the method of calculation and prediction of stability. Small disturbance or Large disturbance;

§ The devices, processes and the time span that must be taken into consideration in order to assess stability : Short term (seconds) or Long term (minutes).

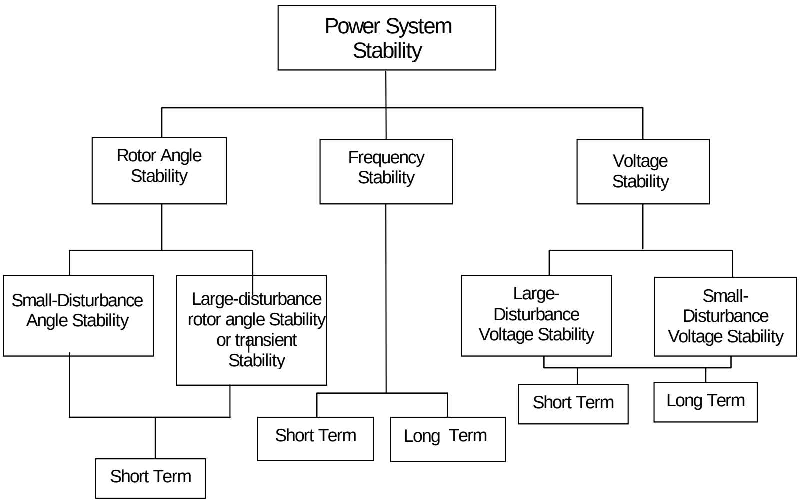


Figure 19: Types of power system stability

- **Rotor angle stability** refers to the ability of synchronous machines of an interconnected power system to remain in synchronism after being subjected to a disturbance. It depends on the ability to maintain/restore equilibrium between electromagnetic torque and mechanical torque of each synchronous machine in the system. Instability that may result occurs in the form of increasing angular swings of some generators leading to their loss of synchronism with other generators. Rotor angle need specific dynamic data, model and tool for TSOs and specific data to be provided for UCTE investigations. The inter-TSOs requirements needed in order to avoid the occurrence of rotor angle instability (inter-area oscillation or loss of synchronism) leading to uncontrolled cascading within the UCTE system are given in the chapter C of the policy 3
- **Voltage stability** refers to the ability of a power system to maintain steady voltages at all buses in the system after being subjected to a disturbance from a given initial operating condition. It depends on the ability to maintain/restore equilibrium between load demand and load supply from the power system. Instability that may result occurs in the form of a progressive fall or rise of voltages of some buses. A possible outcome of voltage

instability is loss of load in an area, or tripping of transmission lines and other elements by their protections leading to cascading outages. Loss of synchronism of some generators may result from these outages or from operation under field current limit. Voltage stability is more local and can be assessed by (quasi-)static analysis. The inter-TSOs requirements needed in order to avoid the local occurrence of voltage stability leading to uncontrolled cascading within the UCTE system are given in the chapter B of the policy 3.

- **Frequency stability** refers to the ability of a power system to maintain steady frequency following a severe system upset resulting in a significant imbalance between generation and load. It depends on the ability to maintain/restore equilibrium between system generation and load, with minimum unintentional loss of load. Instability that may result occurs in the form of sustained frequency swings leading to tripping of generating units and/or loads. The inter-TSOs requirements needed in order to avoid the occurrence of unbalances among loads and generations leading to uncontrolled frequency deviations within the UCTE system are given in the policy 1 & 5.

For more detailed information see:

“Definition and Classification of Power System Stability” Prepared by IEEE/CIGRE Joint Task Force on Stability Terms and Definitions, 9 August 2002