On Secure Interface between Transmission and Distribution Power Networks

Pavel Hering
Faculty of Applied Sciences
University of West Bohemia
Research Centre NTIS
Technicka 8, 306 14 Pilsen
Czech Republic
phering@ntis.zcu.cz

Přemysl Voráč
Faculty of Applied Sciences
University of West Bohemia
Research Centre NTIS
Technicka 8, 306 14 Pilsen
Czech Republic
vorac@ntis.zcu.cz

Petr Janeček
Faculty of Applied Sciences
University of West Bohemia
Research Centre NTIS
Technicka 8, 306 14 Pilsen
Czech Republic
pjanecek@ntis.zcu.cz

Abstract: This paper introduces secure TSO/DSO power flow intervals, in which the transition between transmission and distribution networks are necessarily secure. The growing electricity production in intermittent renewable sources, which are distributed in the network, increases the requirements on ensuring the power network stability and also on providing of ancillary services. Due to the conceivably occurred bottlenecks in the network it may not be possible to use all considered ancillary services. Therefore, it creates the need to define an interface to share information about safe ranges of power transmitted between transmission and distribution networks, for which the secure network operation can be guaranteed.

Key–Words: Transmission Network, Distribution Network, Ancillary Power Reserve, Power system Security.

1 Introduction

Efforts to reduce an amount of produced carbon dioxide emissions and fears of nuclear power has led to significant changes in the way of electricity power production. Whereas in the past, the power was produced mainly in big nuclear and coal-fired power stations connected directly to the transmission network. Nowadays, the increasing portion of energy is produced from small renewable sources, which are connected to distribution networks. Contrary to the big power plants, the small renewable sources, such as photovoltaic and wind power plants have an intermittent power production depending on actual weather conditions instead of taking into account the requirements given by the connected loads. Moreover, the renewable sources are often built in geographical locations, where the conditions are suitable in terms of production, but may be distant from the consumption. This brings the need to transmit large amounts of energy over long distances from those sources to the load centers. This new state caused changes of power flows between transmission and distribution networks. Another aspect affecting power flows is liberalization of the energy market.

Despite the above mentioned changes in power network operation, the transmission system operator (TSO) still purchases and activates ancillary services only on the basis of an imbalance between generation and demand at the lowest price regardless on its origin [1]. This may result in a situation, in which some ancillary services could not be activated due to possible violations of security constraints. To make this operation technically feasible, additional redispatch or reconfiguration have to be done at first. Therefore, there is a greater need to monitor a risk associated with operational actions that may violate security limits.

Nowadays, a series of optimization tools for the calculation of optimal power flow (OPF) exist. These tools help TSOs to find a new operating point of the system either by reconfiguration or redispatch [2, 3]. Nevertheless, these methods compute optimal solution for only one given operating scenario. Uncertainty connected with power demand and generation from renewable sources requires to calculate OPF for several possible scenarios, which would be computationally intensive. Moreover, such point solutions do not provide information how far from a security margin they are. Thus the operator may bring the system to a secure but a fragile state close to the security margin. Probabilistic load flow tools can be used to investigate consequences of deviations from the proposed operating points [4, 5], nevertheless, their complexity makes integration into optimization frameworks difficult. Therefore, a secure interface defining safe operating regions between two transmission networks, transmission and distribution network and or between

two distribution networks is proposed.

The need to define a secure interface is a subject of discussion in the European Planning Standards and Connection Codes of the ENTSO-E. In this paper, the secure interface will be defined in terms of intervals of secure injections (ISI) for each node of the network [5, 6, 7], where computed secure intervals define injection limits, within which a redispatch may be performed without the coordination with other network operators.

The remainder of the paper is organized as follows. In Section 2, power network model and corresponding variables are defined. Formulation of interface for secure power injections is given in Section 3. In Section 4, a method for calculation of intervals of secure injections is introduced. Concluding remarks are presented in Section 5.

2 Power network model

Let the power network model be introduced by a graph with n nodes, where nodes represent potential loads and generating units, respectively, and branches denote transmission or distribution lines or transformers. Further, let us define a finite set $\mathcal{N}$ of the nodes indexed from 1 to n as

$$\mathcal{N} = \{1, \ldots, n\}, \tag{1}$$

where index 1 is reserved for the slack bus, in which the voltage is held constant and the injected power is adjusted to meet the network imbalance. Subsequently, a set of all branches $\mathcal{B}$ is defined as a subset of Cartesian product of set $\mathcal{N}$ with itself, i.e.

$$\mathcal{B} \subseteq \mathcal{N} \times \mathcal{N}. \tag{2}$$

A set of indices of all possible network topologies $\mathcal{T}$ is given as

$$\mathcal{T} = \{0, \ldots, t\}, \tag{3}$$

where the index equal to 0 denotes nominal network topology. For a given topology $\tau \in \mathcal{T}$ it holds $\mathcal{B}_\tau \subseteq \mathcal{B}$.

The set of all nodes $\mathcal{N}$ excluding the slack bus will be divided into a subset of controllable injections $\mathcal{G}$ with cardinality g (e.g. generators providing ancillary services), and a subset of uncontrollable injections $\mathcal{L}$ with cardinality $l = n-g-1$, for which the following relations hold

$$\mathcal{L} \cap \mathcal{G} = \emptyset, \tag{4}$$
$$\mathcal{L} \cup \mathcal{G} = \mathcal{N} \backslash \{1\}. \tag{5}$$

As it is assumed that the network is operating under normal conditions, i.e. the currents and voltages between the individual phases are balanced [8], the single phase model is applicable.

Each node $k \in \mathcal{N}$ is associated with voltage $V_k \in \mathbb{C}$ and power injection $P_k + iQ_k$, where i is the imaginary unit, and each branch $b \in \mathcal{B}$ is associated with a current $I_b \in \mathbb{C}$. For the needs of secure interface formulation, the real and imaginary parts of vector of all nodal voltages $V = (V_k)_{k=1}^n$ and power injections will be placed separately into the real-valued vectors

$$X = (\mathrm{Re}(V), \mathrm{Im}(V)), \tag{6}$$
$$Z = ((P_k)_{k=1}^n, (Q_k)_{k=1}^n),\ k = 1, \ldots, n, \tag{7}$$

where $\mathrm{Re}(V)$, $\mathrm{Im}(V)$ represents real and imaginary of complex value V, respectively.

Let the network has a nominal operating point $x_0 \in \mathbb{R}^{2n}$ representing expected network state for a given planning horizon defined by voltage vector X, which is fixed for all topologies. Then, the reached state at the end of this horizon is defined in terms of deviations $\Delta \in \mathbb{R}^{2n}$ from the nominal operating point such that

$$X = x_0 + \Delta, \tag{8}$$

where from the definition of slack bus $\Delta_1 = \Delta_{n+1} = 0$.

TSO or DSO hold the nodal voltages within a given limits x^- and x^+ to prevent voltage quality issues. A set $\mathcal{Y}_S \subseteq \mathbb{R}^{2n}$ of admissible nodal voltages for which it holds that

$$\mathcal{Y}_S = \left\{X | x^- \leq X \leq x^+\right\}, \tag{9}$$

is defined as the network operating domain.

Another security constraint, which should be taken into account, represents the current in power lines. Such a set of nodal voltages where the constraints on maximum permissible current i_b^+ are met is defined as the security domain $\mathcal{X}_S$, i.e.

$$\mathcal{X}_S = \left\{X \mid |I_b(X)| \leq i_b^+,\ \forall b \in \mathcal{B}\right\}. \tag{10}$$

Finally, the relation between power injections and nodal voltage at the k-th node is as follows [9]

$$P_k = Z_k = X^{\mathrm{T}} \mathbf{Y}_k X, \tag{11}$$
$$Q_k = Z_{k+n} = X^{\mathrm{T}} \mathbf{Y}_{k+n} X, \tag{12}$$

where matrices $\mathbf{Y}_k$, $\mathbf{Y}_{k+n}$ are defined as

$$\mathbf{Y}_k = \begin{pmatrix} e_k \mathrm{Re}(y_k) & -e_k \mathrm{Im}(y_k) \\ e_k \mathrm{Im}(y_k) & e_k \mathrm{Re}(y_k) \end{pmatrix}, \tag{13}$$

$$\mathbf{Y}_{k+n} = \begin{pmatrix} -e_k \mathrm{Im}(y_k) & -e_k \mathrm{Re}(y_k) \\ e_k \mathrm{Re}(y_k) & -e_k \mathrm{Im}(y_k) \end{pmatrix}, \tag{14}$$

with standard basis vectors $e_k \in \mathbb{R}^n$, $k = 1, \ldots, n$ and k-th row y_k of admittance matrix $\mathbf{Y}$.

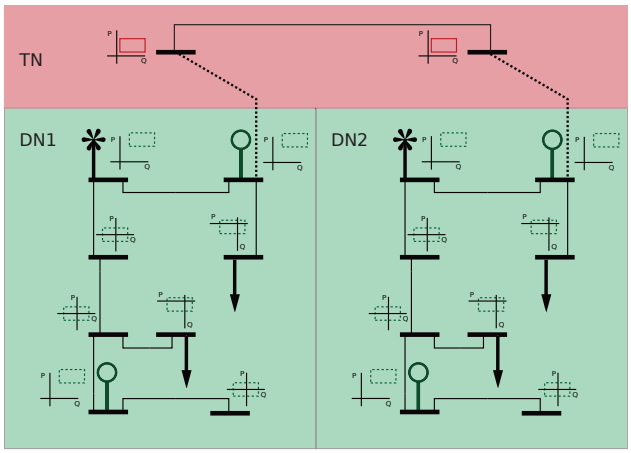

Figure 1: Example of connection of two distribution networks (DN) with transmission network (TN)

3 Secure interface formulation

Let us consider that the power network is monitored by a Wide Area Monitoring System (WAMS) providing synchronous measurements of voltage and current phasors, from which actual nodal injections can be calculated. Depending on possible injections connected to the buses, theoretical ranges of active and reactive powers on each bus can be determined, e.g. as it is shown in Figure 1. Nevertheless, there is no guarantee that all of these power injections will satisfy network security constraints.

Obviously, both systems interact with each other. However, because a socioeconomic impact of possible collapse of transmission network would be much greater than an outage of a smaller distribution network, it is appropriate to reflect this fact when designing the interface and proceed with the establishment of safe limits hierarchically from the highest level (transmission network) down to local networks. The aim of secure interface, therefore, is to provide information to the distribution network operator about the power range, in which he can operate without negative impacts on the transmission network. Similar principles hold between distribution networks and local distribution networks.

Security constraints consist mainly of nodal voltage constraints and line current constraints, however, system operators operate with active (P) and reactive (Q) power. Therefore, it is necessary to transform these constraints to the P-Q space, see Figure 2. As it is a non-convex transformation, the secure domain in P-Q space can be absolutely general and the task of finding its boundary is in fact not easily solvable and, therefore, some approximation has to be done to ensure that the problem will be tractable. A promising approach how to find maximum intervals of secure

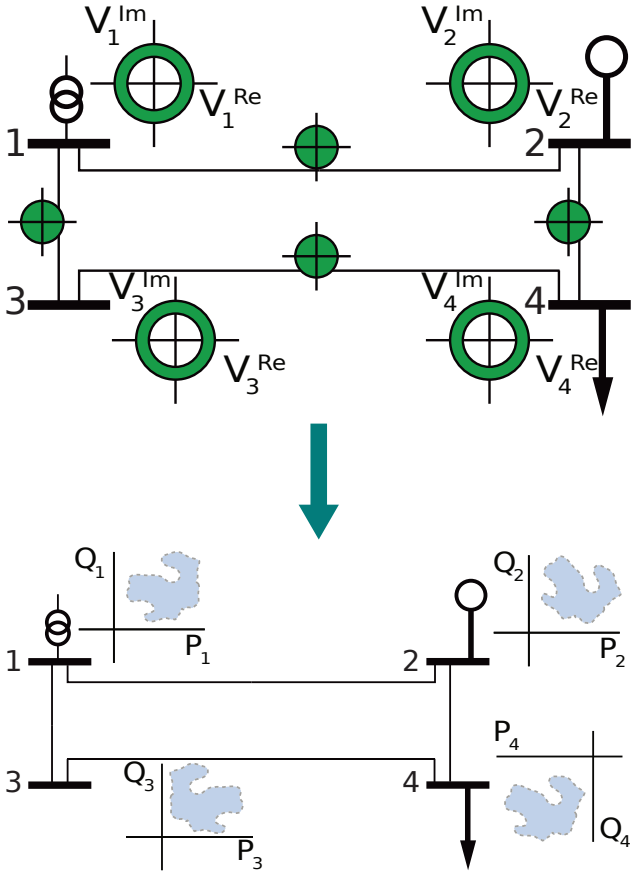

Figure 2: Transformation of security constraints $\mathcal{X}$-space into the P-Q space.

active and reactive power injections at nodes on interface between power networks seems to be a method proposed in [5, 6, 7], which will be briefly introduced in the next section.

4 Maximum intervals of secure power injections in network interface

This section formulates an optimization problem, which determines the maximum intervals of power injections in interface between power networks under consideration of given security constraints.

At first, let us define a set of uncontrollable power injections at nodes $\mathcal{L}$ as follows

$$\mathcal{Z}_L = \left\{ (P_\mathcal{L}, Q_\mathcal{L}) \,\middle|\, (P_k, Q_k) \in [z^-, z^+],\ k \in \mathcal{L} \right\}, \tag{15}$$

where the bounds $z^-, z^+ \in \mathbb{R}^2$ are assumed to be known.

The aim is to find a set of secure injections $\mathcal{Z}_G^*$

satisfying the following optimization problem

$$\begin{aligned}
\mathcal{Z}_G^* &= \arg \max_{z_k^-, z_k^+, T_k} \mu(\mathcal{Z}_G), \\
&s.t. \\
\mathcal{Z} &= \left\{(P,Q) \,\middle|\, (P_{\mathcal{G}}, Q_{\mathcal{G}}) \in \mathcal{Z}_G, (P_{\mathcal{L}}, Q_{\mathcal{L}}) \in \mathcal{Z}_L\right\}, \\
\mathcal{Z}_G &= \left\{(P_{\mathcal{G}}, Q_{\mathcal{G}}) \,\middle|\, (P_k, Q_k) \in [z^-, z^+],\ k \in \mathcal{G}\right\}, \\
\mathcal{Z} &\subseteq \left\{Z \middle| \exists X \in \mathcal{Y}_S, Z_k = X^{\mathrm{T}} \mathbf{Y}_k X, \right. \\
&\qquad \left. k = 1, \ldots, 2n\right\} \Rightarrow \\
\mathcal{Z} &\subseteq \left\{Z \middle| \exists X \in \mathcal{X}_S, Z_k = X^{\mathrm{T}} \mathbf{Y}_k X, \right. \\
&\qquad \left. k = 1, \ldots, 2n\right\}. \qquad (16)
\end{aligned}$$

The optimization problem (16) is not easily solvable hence the following simplifying assumptions are defined:

A1 $\mathcal{X}_S = \left\{X \middle| X = x_0 + \Delta, \mathbf{D}\Delta \leq d\right\}$, i.e. the network security domain is taken to be a bounded convex polytope, where $\Delta_1 = \Delta_{n+1} = 0$.

A2 The network operating domain $\mathcal{Y}_S$ is described by the Cartesian product of intervals $[x_k^-, x_k^+],\ k = 1, \ldots, 2n$, and the system operator holds nodal voltages in the network operating domain.

A3 The injections are expanded around the nominal operating point x_0 and divided into affine terms and purely quadratic terms.

For more detailed information about the ISI method see e.g. [5, 6, 7].

5 Conclusion

The paper discussed the need to define secure interface among different power networks, mainly between the transmission networks and distribution network in liberalized energy market and increasing amount of energy produced in intermittent renewable energy sources. There was recommended hierarchy in seeking of secure power intervals from the highest to the lowest level. As a suitable tool for computing the intervals of secure injections was suggested the ISI method.

Acknowledgements: The work was supported by project PUNTIS-LO1506 and Technology Agency of the Czech Republic under project TE01020197.

References:

[1] B. Kirby, *Ancillary services: Technical and commercial insights,* Wartsila, Tech. Rep., 2007.

[2] L. Platbrood, H. Crisciu, F. Capitanescu, and L. Wehenkel, Solving very large-scale security-constrained optimal power flow problems by combining iterative contingency selection and network compression, *Power system computation conference,* 2011.

[3] K. W. Hedman, R. P. O'Neill, E. B. Fisher, and S. S. Oren, Optimal transmission switching with contingency analysis, *IEEE Transactions on Power Systems*, 2009.

[4] J. M. Morales and J. Perez-Ruiz, Point estimate schemes to solve the probabilistic power flow, *IEEE Transactions on Power Systems*, 2007.

[5] E. Janeček and D. Georgiev, Probabilistic extension of the backward/forward load flow analysis method, *IEEE Transactions on Power Systems,* 2012.

[6] D. Georgiev, E. Janeček, and P. Voráč, Computing intervals of secure power injection, *in Proceedings of the 19th IFAC World Congress,* 2014.

[7] P. Voráč, E. Janeček, and D. Georgiev, Interval based network operation respecting n-1 security criterion, *in Innovative Smart Grid Technologies Conference Europe (ISGT-Europe),* 2014 IEEE PES, Oct 2014, pp. 1–6.

[8] J. J. Grainger, W. D. Stevenson, JR. *Power System Analysis*, McGraw-Hill, Inc., 1994.

[9] J. Lavaei and S. H. Low, Zero duality gap in optimal power flow problem, *IEEE Transactions on Power Systems*, 2012.