Use Case Summary – Voltage Control in Medium Voltage Grid

The primary aim of this use case is to address the communication needs of a Voltage Control function for medium voltage grids connecting Distributed Energy Resources (DERs). The actions derived from the Voltage Control function are considered with the specific aim of defining an ICT architecture suitable for the security analysis. The Medium Voltage Control is a didactic case for illustrating the need of cyber security in smart grid applications, first because its behaviour influences both the system operation and economy, secondly for the high level of inter-networking of its ICT architecture. The evaluation of attack processes to the Voltage Control function is aimed at identifying security controls to counter act those attacks having the capability of compromising the voltage profile.

The connection of DERs to medium voltage grids can influence the status of the whole power grid: the behaviour of DERs can affects the capacity of the DSO (Distribution System Operator) to comply with the contracted terms with the TSO (Transmission System Operator) and directly the quality of service of their neighbour grids.

The main functionality of the medium voltage control function is to monitor the active distribution grid status from field measurements and to compute optimized set points for DERs, flexible loads and power equipment deployed in HV/MV substations.

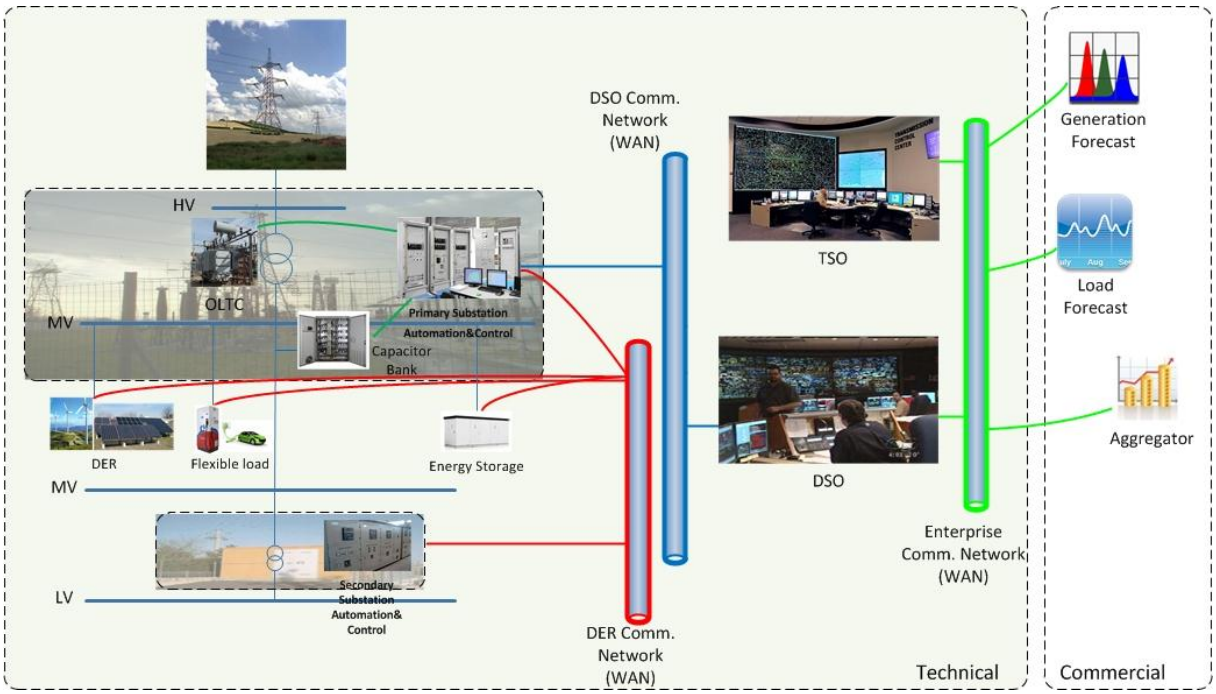

Figure 1 Overview of Medium Voltage Control Use Case

The optimization function is performed by a Medium Voltage Controller of a HV/MV substation control network. In order to pursue the previously defined objective, the Controller calculates in a coordinated manner the optimal states of the controllable devices across the substation area.

The control strategy requires information originating externally to the DSO domain. From the operation stand point, the optimization function has to receive voltage regulation requests by the TSO whenever a transmission grid contingency needs to apply preventive measure to voltage collapse. Load and generation forecasts are used to optimize the operation of distributed devices, while the economic optimization is based on market prices and DER operation costs.

A first major design assumption underlying the use case ICT architecture is that communications from the DMS (Distribution Management System) application in the DSO centre provide to the Controller the information related to DER features, changes in the grid topology, requests by TSO, load/generation forecasts and market data. This design choice preserves the integrity of the distribution grid operation by limiting the communication channels at the substation level and concentrating the communications with those external actors at the DSO centre level.

The control loop is triggered by critical events (e.g. under/over voltage event, TSO request, grid topology change). In absence of criticalities, the VC function is executed on a periodic base (e.g. every 15 minutes) for optimization purposes. The total response time of its closed control loop, from the start of the elaboration to the end of the set point actuation, depends on actuation time constants of OLTC and DER power electronics.

The architectural layout deployed for implementing the VC function depends on the responsibilities attributed to the use case roles and on country-based regulations. According to the architectural layout in Figure 1, the data supply chain of the VC function depends on several communication links enabling remote accesses from systems outside the perimeter of the DSO operation. The DMS application in the DSO centre has permanent links (the green WAN in Figure 1) with four actors (TSO, Aggregator, Generation Forecaster and Load Forecast); the Controller in the DSO substation has permanent communication links (the red WAN in Figure 1) with third party DERs, possibly deploying heterogeneous communication technologies available in different geographical areas; communications between DMS and substation automation and control systems pass through the DSO SCADA links (the blue WAN), possibly based on telco services. By focusing on the core of the VC scheme, it results evident that the correct elaboration of the optimal set points depends on the provision of correct operation and economic data from the above communication channels. A malicious attack to one of the above communication links may cause either the loss of input data (generation forecasts, economic data from the Aggregator, TSO requests, topological changes), or the introduction of faked input values or output set points. The effects of such communication attacks may lead the control function either to diverge from optimum set points or, even worst, to produce inadequate set points with cascading effects on connected generators. The global impact of cyber attacks to the Voltage Control functions on the supplied power depends on the grid size, the amount of distributed generation, the control network topology on the top of the power grid structure and the extension of the attack.