IMPACT OF DER INTEGRATION ON THE CYBER SECURITY OF SCADA SYSTEMS – THE MEDIUM VOLTAGE REGULATION CASE STUDY

Giovanna DONDOSSOLA
RSE – Italy
dondossola@rse-web.it

Fabrizio GARRONE
RSE – Italy
garrone@rse-web.it

Gianluigi PROSERPIO
RSE – Italy
proserpio@rse-web.it

Carlo TORNELLI
RSE – Italy
tornelli@rse-web.it

ABSTRACT

The operation of active distribution grids with high penetration of Distributed Energy Resources, connected to Medium Voltage bars and feeders, requires the implementation of new Medium Voltage regulation functions. Assuming that this control function is best positioned in the primary substations of the control hierarchy, the paper presents the architectural changes occurring at both the centre and the substation control levels. Possible cyber risk scenarios and mitigation countermeasures of the new SCADA architecture are discussed, in compliance with the IEC communication standards and the IEC/NIST cyber security technical recommendations related to the smart grid sector.

INTRODUCTION

The integration of DER (Distributed Energy Resource) technologies into distribution grids poses several challenges to the evolution of the actual SCADA (Supervision Control And Data Acquisition) infrastructures supporting the management and operation of the Medium Voltage grids.

Following a centralized approach to operation adopted in passive distribution grids, nowadays the control of HV/MV (High Voltage / Medium Voltage) substations is remotely performed through the DMS (Distribution Management System) located in geographical area Control Centers which are connected via a private IP network with all supervised substations. In order to protect the power process as much as possible all the data communications with the external systems are concentrated in the Control Centre, while the peripheral Substation Automation Systems mainly implement communications towards the Control Centre, with the exception of a few, very limited, inter-substation communications.

With the penetration of (possibly third party) active DERs (such as generators, flexible loads, and energy storages) connected to MV bars and feeders, it is necessary to analyze the upgrade to current SCADA systems required by the operation of these active distribution grids.

In this paper the MV regulation is used as a sample case study for designing an extended control architecture taking into account legacy issues. According to a system oriented view of the MV regulation case, the paper discusses the major architectural challenges including the interactions with both the market participants – more related to the energy economy – and the grid operation main actors – more related to the technical constraints of the electrical system. The design choices at the different layers of the smart grid architecture (i.e. function, information, communication, component and security) are conditioned by the legacy aspects from the existing control infrastructure.

Section 1 introduces the MV regulation function and its associated information flows, assuming that this control function is best positioned at the substation level.

Section 2 presents the architecture implementing the use case. In the solution proposed, ICT (Information and Communication Technology) architectural changes occur at both the centre and the substation levels.

In section 3 the paper discusses cyber risks and mitigation countermeasures of the DSO (Distribution System Operator) SCADA architecture incorporating the control and communication extensions required by the MV regulation function in active distribution grids.

1. USE CASE – MV REGULATION

In MV feeders including distributed generation, the power injected by DERs can lead the voltage beyond the limits in some parts of the grid, mainly due to uncontrollable generation from renewable sources. Control actions limited to the OLTC (On Line Tap Changers) of the substation transformers, as usually operated in passive grids, may be not sufficient to meet the supply requirements established by the norm EN 50160. Voltage profiles in the MV grids may be adjusted acting also on DERs connected to the MV feeders and other components in the substation as capacitor banks and storage devices.

The sequence diagram in Fig. 1 shows the information exchanges of the MV regulation function, distinguishing the actors involved in its communication flows. The control strategy requires information originating externally to the DSO domain. From the operation stand point, the optimization function has to receive voltage regulation commands by the TSO (Transmission System Operator) whenever a transmission grid contingency needs to apply preventive measure to voltage collapse (flow n.1). Load and generation forecasts (flow n. 4) are used to optimize the operation of distributed devices, while the economic optimization is based on market prices and DER operation costs (flow n. 5).

A first major design assumption underlying the control strategy in Fig. 1 is that asynchronous (event-based) communications from the DMS application in the DSO

centre provide to the MV regulation function the information related to DER features, the changes in the grid topology and the information by TSO, forecaster and market. This design choice preserves the integrity of the distribution grid operation by limiting the amount of communication channels at the substation level and concentrating the communications with those external actors at the DSO centre level.

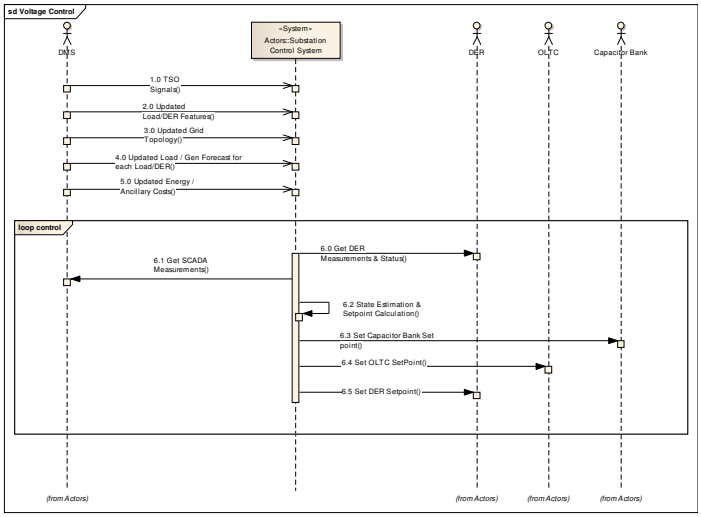

Fig. 1**. MV Regulation - Control strategy**

The main control loop of the MV regulation is based on intra-substation and substation-DER communications. Given the grid topology, field measurements, market prices and resource operation costs, the voltage control function regulates the voltage profile computing and sending appropriate set points to the third party distributed energy resources (generators, flexible loads and storages) and distributor's devices (i.e. capacitor banks and OLTCs). The algorithm is based on an AC Optimal Power Flow where grid losses and integral constraints are taken into account. The status of the grid, required by the control algorithm, is computed by a State Estimator function, based on actual measurements and grid topology. At the actual stage of the use case design the State Estimator is assumed to be a standalone sub-function of the MV regulation algorithm and does not require communicating with the Control Centre.

The control loop is triggered by critical events (e.g. under/over voltage event, TSO request, grid topology change). In absence of criticalities, the regulation 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 the time constants of the power electronics of distributed generators. As the OLTC has a time constant of 3 seconds for set point actuation, it seems reasonable to assume that the total time response of the MV regulation is of the order of decades seconds.

2. ARCHITECTURAL CHALLENGES

The implementation of MV regulation strategy described above introduces architectural extensions to the DSO SCADA systems at both the centre and the substation layers. Fig. 2 shows the main components of the extended architecture.

By focusing on the HV/MV substation, this use case highlights the need of a new station level control IED (called Station Computer) executing the VPC (Voltage and Power Control) algorithm on the basis of the incoming communications from the DMS and DER SCADA, and the outcome of the State Estimator. It produces set points dispatched towards the IEDs controlling the substation devices (OLTCs and capacitor banks) and the DERs**.**

New communication functions are introduced at different intra-substation architectural levels. At the process layer, components like the OLTC Controllers and the Capacitor Bank Controllers have to be extended with communications to/from the Station Computer. At the station layer, a second major design choice is required for the implementation of the communications from/to the Station Computer to/from the remote entities.

A first architectural solution, minimizing the impact in term of installation costs, consists in extending the existing substation gateway serving the communications with the DSO Control Centre with additional links communicating with external DERs. A second solution (shown in Fig. 2) is based on the deployment of a separate gateway allowing the physical decoupling of the communications with the Control Centre from those with DERs. As these two types of external links provide different security assurances, this second solution, though more expensive in terms of installation costs, is more convenient when the cyber security risks are evaluated, as synthetically explained in

the following section.

With reference to the evolution of standard protocols in SCADA communications, the information exchanges of the MV regulation function would map onto the IEC 60870-5-104 protocol (for centre-substation communications) and the MMS profile of the IEC 61850 standard (for the intra-substation and substation-DER communications). Both these application protocols are based on standard client/server TCP/IP connections.

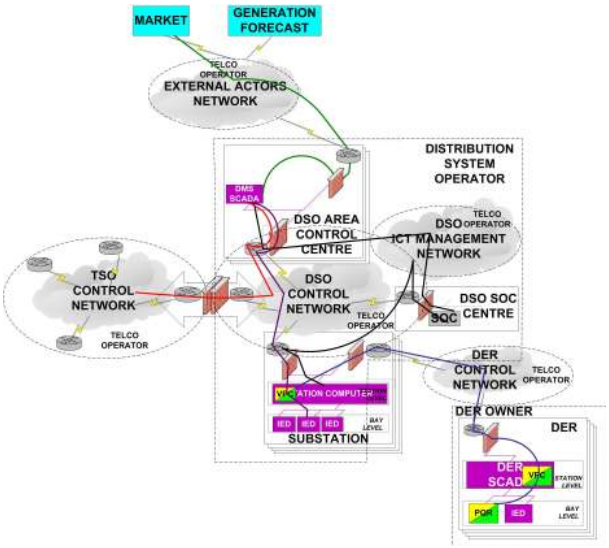

Fig. 2. ICT architecture

3. CYBER SECURITY

No standard methodology for conducting cyber risk assessment of energy control systems is available, while the IEC and NIST recently published, respectively, a Roadmap [1] and a Guideline document towards the standardisation of cyber security in smart grids [2]. Smart grid applications, like the MV regulation case discussed in the paper, are characterised by distributed ICT architectures whose internetworking is based on open communication technologies exposed to a plethora of cyber threats. Therefore the cyber security analysis of their communication flows becomes essential to develop secure ICT architectures integrating appropriate protections to networking risks.

In this section a two step approach to the security analysis of the MV regulation case is followed, as a practical mean for sharing the basic principles underlying the analysis of cyber security in smart grid ICT architectures.

In the first step the *consequence severity* of the communication malfunctions on the MV regulation and on the system operation and economy are evaluated, at the aim of deciding the minimum security controls required by the criticality level of the control function.

The second step analyses the system topology for deriving possible compromise paths of attack vectors to the secure architecture at the aim of evaluating residual risks and identifying additional security measures for unacceptable risks [4].

Step1 – Essential security controls

The MV regulation 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. According to the architectural layout in Fig. 2, the supply chain of the MV elaboration function depends on several communication links involving remote accesses from systems outside the perimeter of the DSO organisation:

- the DMS application in the DSO centre has permanent links with three third parties (market, generation forecaster and TSO);
- the MV regulation application in the DSO substation has communication links with third party DERs, possibly deploying heterogeneous communication technologies available in different geographical areas;
- the wide area links supporting the new inter-organisation information exchanges and the existing DSO SCADA links between DMS and substation automation systems may be based on third party connections from telecommunication service providers.

By focusing on the core of the MV regulation 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. However a malicious attack to one of the above communication links may cause

- the loss of generation forecasts, economic data from the market, TSO requests, topological changes, operational data from the DMS
- the introduction of faked generation forecasts, economic data from the market, TSO requests, topological changes, operational data from the DMS
- the introduction of faked set points.

The effects of communication attacks may lead the regulation function either to diverge from optimum set points or, even worst, to produce inadequate set points with cascading effects on connected generators.

Given the high severity of the communication malfunctions, the following security requirements to the MV regulation communications are identified:

- continuous *availability* of all the permanent communication links for the transmission of monitoring data and asynchronous (events and commands) messages;
- *authenticity* and *integrity* of sending and receiving data streams. The MV regulation algorithm requires the *undisturbed* execution of

acquisition and actuation sequences based on *ordered* flows of status, events and commands.

In order to meet the most critical cases, the final objective of the security countermeasures for the MV regulation case is to undo data losses and spurious data. Any corrective recovery action mitigating the effect of communication anomalies has to satisfy the response time requirements of the MV regulation application assumed to be of order of decades seconds.

Given the above security requirements, the following preventive controls are considered essential for defending the communications of the MV regulation case:

- All the security domains (substations, DERs, DSO centres, TSO, market, generation forecaster) have to apply strict network access control policies through appropriate filtering technologies;
- All the communication flows have to be authenticated and encrypted through appropriate security technologies. According to the security standard IEC 62351 – Part 3 [5], the SCADA and telecontrol protocols that make use of TCP/IP as a message transport layer have to be protected by specific TLS (Transport Layer Security) configurations applicable to the telecontrol environment. Wide area communications have to be protected by standard IPSEC Virtual Private Networks.

With the introduction of the above security controls, the management and administration of the ICT components justifies the setup by the DSO of a central SOC (Security Operation Centre in Fig. 2) that may be operated by a third party service provider. The data flows for the remote management of communication and control devices have to be implemented in a secure way for avoiding that cyber risks of the ICT operations propagate to the most critical grid operations. The outsourcing of security services, as also the existence of inter-organisation links, requires establishing precise contractual obligations to guarantee that appropriate organisational and technical measures are applied to all the third party remote accesses. However, as explained in the second step of the analysis, the setup of a SOC operated by the utility itself is definitely considered visionary in the management of smart grid cyber security.

Step 2 – Analysis of residual risks

The ICT architecture extended with network security measures still suffers of residual cyber risks due to possible attack vectors [4]. Attack vectors are characterised by specific attack techniques compromising the information flows along pathways towards the attack targets.

Aimed at assuring end-to-end security along all the communication pathways in the ICT architecture, the second step focuses on analysing possible attack vectors from remote accesses to the VPC target. Indeed according to [3] attack modelling is a valuable approach to follow for conducting such a residual risk assessment.

The evaluation of the effects of specific attack processes to the MV regulation function has a double role: on one side it allows evaluating the success probability of a given type of attack process and its actual capability of compromising the MV voltage profile; on the other side it allows identifying additional security controls to counter act specific types of attack processes. The most serious attacks are represented by intrusion processes able to manipulate the TCP/IP information flows for introducing faked inputs data and/or output set points to the MV regulation function. In order to mitigate the effects of complex intrusions, the SOC should be extended with security monitoring tools generating alerts from protocol and system logs. From the stand point of attack vectors, the MV regulation architecture in Fig. 2, decoupling the links of the DSO SCADA from the links with external systems, allows a isolation of the attack effect along the information supply chain.

CONCLUSIONS

The paper presented the basic criteria underlying the analysis of cyber security for smart grid applications. A two step analysis process has been applied to the MV regulation case, one of the most critical functions towards the active operation of distribution grids. The main lesson learned from this exercise is that different architectural solutions determine different cyber-power risks which have to be carefully assessed through targeted experiments.

REFERENCES

[1] IEC, 2010, “IEC Smart Grid Standardization RoadMap”, SMB Smart Grid Strategic Group SG3, Edition 1.0, June 2010.

[2] NIST Internal Report 7628, “Guidelines for Smart Grid Cyber Security”, 3 Volumes, The Smart Grid Interoperability Panel – Cyber Security Working Group, August 2010.

[3] G. Dondossola, L.P. Cambacedes, J. McDonald, M. Ekstedt, A. Torkilseng, 2011, “Modelling of cyber attacks for assessing smart grid security”, *Proceedings Cigré D2 2011 Colloquium,* Buenos Aires 19-20 October 2011.

[4] G. Dondossola, F. Garrone, J. Szanto, “Cyber risk assessment of power control systems – A metrics weighted by attack experiments” 2011 IEEE PES General Meeting, Detroit, Michigan 24-28 July 2011.

[5] IEC 62351 “Power systems management and associated information exchange - Data and communications security” Parts 1-10.