ARTICLE IN PRESS

Sustainable Energy, Grids and Networks xx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

Sustainable Energy, Grids and Networks

journal homepage: www.elsevier.com/locate/segan

Impact of cyber-physical system vulnerability, telecontrol system availability and islanding on distribution network reliability

Q1 S. Conti, A. La Corte, R. Nicolosi, S.A. Rizzo *

University of Catania - D.I.E.E.I., Italy

ARTICLE INFO

Article history:
Received 10 November 2015
Received in revised form
4 March 2016
Accepted 17 March 2016
Available online xxxx

Keywords:
Cyber-physical systems
Distributed power generation
Microgrid
Power distribution
Power system reliability
Smart Grid

ABSTRACT

The addition of telecontrolled and automated sectionalizers along the distribution network has permitted to speed up fault location procedures to reduce the restoration time. Nowadays, some utility are installing circuit breakers (CBs) along the network to reduce the average number of customers' outages too, but the use of time selectivity strongly limits the number of CBs installed in topological sequence. In Smart Grid perspective, a protection system upgrade towards telecontrolled CBs allowing to overcome this limitation is expected, and, more in general, a transition towards a cyber-physical system (CPS) implementing protection schemes based on telecontrolled switches only. Moreover, Smart Grids should allow to exploit the potential benefit deriving from autonomous microgrids in terms of service continuity. This work presents an analytical formulation to assess the impact of CPS vulnerability and centralized telecontrol system availability on system reliability in networks where islanding is permitted by regulation. The formulation is applied to a realistic case study. The results have shown that islanding effectively reduces the outage duration even when the CPS is very vulnerable. On the other hand, islanding is able to strongly reduce the outage rate too when the CPS security level is high.

1. Introduction

Q2 Smart Grid systems (SGSs) [1] have been widely investigated since they are the enabling key for a high penetration of distributed Q3 generators (DGs), especially based on renewable energies [2]. The growing world-wide environmental concerns and the shortage of primary energy resources are the main drivers towards a broad diffusion of renewable generators [3]. Research activities on SGSs are mainly focused on solving major technical issues due to the presence of DGs in electrical distribution networks, such as voltage and frequency control, voltage flicker, harmonics, power flow inversion, non-intentional islanding, increased fault currents, protections miscoordination, incorrect reclosers operation, etc. [4–6]. DGs can be turned into a resource for the network as they can improve service continuity and voltage regulation, decrease line power losses, lower energy price by means of demand-responds mechanism, reduce pollution thanks to a large penetration of green generators [7].

To face these complex tasks, the distribution system must be associated to a cyber-system to exchange and analyze real-time information in order to operate the network by using different communication resources as well as control and automation systems [8,9]. Moreover, such a cyber system enables to exploit the potential positive impact on system reliability of autonomous microgrids (intentional islands) supplied by local DGs [10]. Also, a cyber infrastructure where telecontrolled circuit breakers (CBs) and sectionalizers are installed along the distribution network improves the distribution system reliability by reducing the network portions affected by a fault and/or by quickly sectionalizing the faulted region [11–16] both when islanding is permitted or not by regulation. More specifically, when islanding is not permitted by regulation, the average number and cumulative duration of interruptions per customer is reduced by opening the telecontrolled CB closest to the fault, thus avoiding to disconnect the upstream customers. Moreover, the average cumulative duration is further reduced by means of telecontrolled sectionalizers that, after the fault is cleared by the CB, quickly reduce the network portion affected by the fault. When an alternative path is located downstream from the faulted zone or islanding is permitted by regulation, the load in the network portion downstream from the faulted zone can be transferred or supplied by local generation.

On the other hand, cyber attacks against the SCADA system due to financial gain or terrorism [17] can worsen distribution

* Corresponding author.
E-mail addresses: stefania.conti@dieei.unict.it (S. Conti), aurelio.lacorte@gmail.com (A. La Corte), rosario.nicolosi@gmail.com (R. Nicolosi), santi.rizzo@dieei.unict.it (S.A. Rizzo).

http://dx.doi.org/10.1016/j.segan.2016.03.003
2352-4677/

Please cite this article in press as: S. Conti, et al., Impact of cyber-physical system vulnerability, telecontrol system availability and islanding on distribution network reliability, Sustainable Energy, Grids and Networks (2016), http://dx.doi.org/10.1016/j.segan.2016.03.003

system reliability. For example, in a locally based energy market in Smart Grid enabling multiple microgrids [18], an attacker could be someone who acts in the interests of a DGs' owner in order to hinder the competitors. Generally speaking, an attacker can be considered as a black hat hacker that violates security for little reason beyond maliciousness or for personal gain or also a hacktivist that hacks to promote an ideological, political, religious or social message [19]. In the worst case, the attacker is a cyberterrorist aiming at fearing civil population [19]. In a cyberwarfare perspective, the attacker can be a nation that penetrates foreign nation's networks for the purposes of causing damage or disruption [20]. The way the attackers must follow to conduct a successful attack depends on the working mode of the control system, on the means they command, on their degree of knowledge of the control system, on the system security level and so on. Finally, there are other kinds of cyber attacks, such as cybertampering, which do not affect distribution system reliability but they are of interest for utilities due to economic reasons [21]. In [22] the feasibility of cybertampering on electronic meters is considered, its evolution in a distributed form is discussed in [23]. When a successful cyber attack affecting distribution system reliability occurs, or when other adverse events occur, such as the control system or telecommunication network being down, the aforesaid improvement in the average number and cumulative duration of interruptions per customer can be drastically limited. More specifically, for safety reasons, a CB protection detecting a fault has to trip when it does not receive any communication by the cyber infrastructure within its delayed operation time. Therefore, the CB installed at the sending end of a PS's feeder may untimely open when one of these adverse events occurs because it detects all the faults in the network.

National Institute of Standards and Technology asks for tools and techniques that provide quantitative notions of risks, that is, threats, vulnerabilities, and attack consequences for current and emerging power grid systems [24]. Therefore, regardless the attacker's motivations, it is important to study and analyze the impact of its attacks on the power system as they could severely affect reliability [8]. In this perspective, the present paper firstly provides the analytical formulation to assess distribution system reliability when a protection scheme only based on telecontrolled switches is considered in networks where islanding mode of operation is not permitted by regulation. In particular, the work investigates the reliability improvement achievable by means of a protection scheme based on telecontrolled switches, logic selectivity and automation for different availability levels of centralized telecontrol system (CTS), also accounting for the possibility of cyber-attacks against a power grid's SCADA system.

The paper also provides the analytical formulation to be adopted to assess the distribution system reliability in networks where islanding mode of operation is permitted by regulation and the aforesaid protection scheme is adopted. In particular, the combined effect of several factors such as DGs' ability to meet island load, availability probability related to a CTS implementing logic selectivity for protection, untimely opening of the primary substation' (PS) circuit breaker and unavailability of automatic restoration procedure due to malicious cyber attacks to the SCADA system [17,25] is investigated. Finally, computing the probability a successful cyber attack occurs, the availability probability of the centralized control system, as well as the estimation of the generation's probability of adequacy in each island, is out of the paper's scope.

2. Reliability assessment

Many reliability indices [26] are computed using the annual outage rate (λ_i) and duration (U_i) related to each customer. These load point (LP) indices can be computed as

$$\lambda_i = \sum_{k}^{N_B} \lambda_{i,k} \quad (1)$$

$$U_i = \sum_{k}^{N_B} U_{i,k} \quad (2)$$

where N_B is the number of branches in the distribution network, $\lambda_{i,k}$ and $U_{i,k}$ are, respectively, LP i annual outage rate and duration due to a fault in branch k, with failure rate f_k (it is usually the average number of faults per year) and repair time t_{Rk} (it is usually the mean time to repair the fault).

In [27] an innovative method has been proposed to assess these indices in two different scenarios, that is islanding mode of operation permitted and not permitted by regulation. One of the main merit of this systematic method is its capability to identify the different ways in which a fault can affect an LP (called *Cases*) in any radial network. On the other hand, it assumes that: several switches can be installed in topological sequence along the network; the CPS enabling the automation systems is invulnerable; a fully reliable communication infrastructure supports a protection scheme exploiting logic selectivity to operate only the switches closest to the fault. Therefore, the effect of telecommunication network unavailability, centralized control system dependability and CPS vulnerability is neglected. However, it is also important to consider that one or more cyber vulnerabilities within the communications and computing devices could be exploited in order to remotely implement a malicious attack to the system [28]. The types of cyber intrusions required to execute an attack, and consequently the realism of the attack, are specific to the actual protocols, software and hardware architecture [29], and, usually, an attack involves data interception, modification and fabrication [28]. Perhaps the most common mechanism to penetrate a trusted perimeter is through a network-based attack vector. Exploiting poorly configured firewalls for both misconfigured inbound and faulty outbound rules is a common entry point, enabling an adversary to insert a malicious payload onto the control system [30]. An attacker can preinstall malicious codes or backdoors into a device prior to shipment, or else an employee (or legitimate user) authorized to access system resources can perform malicious actions [30]. In the last case, the insider have intimate knowledge of the control system working mode as well as defense mechanisms [30]. Therefore, the attacker can successfully inject worms into vulnerable control systems and reprogram them, after that he/she can perform a remote attack from the comfort of its home [30]. Note that, a "smart attack" can be also performed when the attacker has in-depth power system knowledge in order to make more difficult any defence.

Then, the proposed formulation is intended to overcome the aforementioned limitations, by accounting for telecommunication network and centralized control system dependability, as well as for CPS vulnerability in order to enable the distribution system operator (DSO) to optimally plan future Smart Grid based on centralized control to strongly reduce mean annual outage rate and duration for the LPs of the network.

3. Centralized protection scheme implemented by the cyber-physical system

This section considers a Smart Grid scenario where islanding is not permitted and the protection scheme enabled by the CPS is only based on telecontrolled switches. When a fault occurs, firstly the control system has to open the CB (j) closest to the fault and disconnect the DGs located downstream from the opened CB. Then, it has to perform a fault location procedure to open

Please cite this article in press as: S. Conti, et al., Impact of cyber-physical system vulnerability, telecontrol system availability and islanding on distribution network reliability, Sustainable Energy, Grids and Networks (2016), http://dx.doi.org/10.1016/j.segan.2016.03.003