Electrical Power and Energy Systems 101 (2018) 371–384

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

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

# Reliability assessment of a power system with cyber-physical interactive operation of photovoltaic systems

Hasan Gunduz*, Dilan Jayaweera

*Department of Electronic, Electrical and Systems Engineering, University of Birmingham, Edgbaston, Birmingham B15 2TT, United Kingdom*

ARTICLE INFO

*Keywords:*
Cyber-physical threats
Markov chains
Photovoltaic power systems
Power system planning
Power system reliability
Power system operation

ABSTRACT

With an increased transition towards low carbon technologies and their interactions with information and communication technologies (ICT) in a smart grid environment, reliability performance studies should essentially be incorporated with cyber-physical systems interactions. Such an integrated operating environment is inevitably exposed to cyber-physical system threats, particularly, with the increased presence of new and smart components. In the purview of the above, this paper proposes an innovative algorithm to determine the availability and unavailability of cyber physical interactive system components for quantifying the level of risk posed by random cyber threats. This paper also provides the pathway for the power system reliability assessment of a cyber-physical integrated system operation with multiple photovoltaic (PV) system configurations by incorporating Markov-Chain transitions for PV system components. A set of case studies were performed by simulating the cyber-physical integrated operating environments and the results suggest that impacts from cyber threats on interactive PV operation are considerable and a quantitative assessment is required to determine real impacts on a specific power system.

## 1. Introduction

Renewable energy technologies are essential components under climate change policies in many countries, and they play a vital role in decarbonisation efforts. In perspective of generation diversity in energy sector, solar photovoltaic (PV) is amongst the most promising distributed energy resource due to being eco-friendly, sustainable and free of operational cost. A phenomenal increase of 8000 percent has been observed in nominal capacity of solar PV in last two decades [1]. Apart from the benefits and upsurge in PV installations, the stochastic nature of PV system poses challenges to the power system operation. The uncertainties in power generations of PV systems presents distribution and transmission operators with enormous challenges to operate the system with an adequate level of reliability.

Integration of PVs and other renewable technologies in a smart grid has introduced new technological elements. The smart power grid may carry enormous level of information and communication technologies (ICT), including supervisory control and data acquisition (SCADA), advanced metering infrastructure (AMI), and communication control panels, etc. These necessary assets of interconnected power grid are potential targets of cyber-attacks and threats. These attacks, depending on their intrusion level can have adverse effects upon the capability of smart grid monitoring. This can directly or indirectly influence the energy network security, stability, resilience and eventually the overall system reliability [2–4].

Different power systems around the world have already been affected by malwares called Black Energy, Havex and Sandworm [2]. The recent cyber-attack on Ukrainian energy network in 2015 forced governments to consider cyber-attacks as a national energy-security issue and improve the resilience of the power systems [2]. Recent cyber-attacks on Ukrainian distribution grids and electricity utilities demonstrate that ICTs can potentially bring cyber-physical vulnerabilities and damages, sub-system outages, most notably even large-scale black-outs [4]. According to [3] in USA, installation of AMI has reached almost 65 million by 2016, represents 43% of all customers in USA and integration of AMIs are expected to be increased. These deployments evidence that the uncertainties of the working principles of PV systems on the grid, and their relationship with cyber-integrated systems like ICTs are going to increase. Unexpected interruption risks are reshaping future grid planning and operation as a defensive operating platform. This important and necessary attention on interconnected grids introduces questions for example, how will energy providers, consumers and

*Abbreviations:* AMI, advanced metering infrastructure; CPS, cyber-physical system; ES, ethernet switch; DER, distributed energy resource; ICT, information and communication technology; MU, merging unit; PV, photovoltaic; RBTS, Roy Billinton Test System; SCADA, supervisory control and data acquisition

* Corresponding author.
*E-mail addresses:* hxg461@bham.ac.uk (H. Gunduz), d.jayaweera@bham.ac.uk (D. Jayaweera).

https://doi.org/10.1016/j.ijepes.2018.04.001
Received 25 October 2017; Received in revised form 16 March 2018; Accepted 2 April 2018
0142-0615/ 

**Nomenclature**

$A$, $U$ the system indicators (availability/unavailability)
$P_{f_X}$, $P_{r_X}$ failure/recovery state probability of component X (series)
$\lambda_{system}$, $\mu_{system}$ failure/recovery rate of system
$\lambda^k_{Panel}$, $\mu^k_{Panel}$ failure/recovery rate of kth PV panel
$\lambda_{CC}$, $\mu_{CC}$ failure/recovery rate of charge controller
$\lambda_{BB}$, $\mu_{BB}$ failure/recovery rate of battery bank
$\lambda_{MI}$, $\mu_{MI}$ failure/recovery rate of micro-inverter
$\lambda_{String_k}$, $\mu_{String_k}$ failure/recovery rate of kth string
$P^X_{f_{String}}$, $P^X_{r_{String}}$ failure/recovery state probability of component X (parallel)
$\lambda_{Cyber}$, $\mu_{Cyber}$ failure/recovery rate of cyber-physical system
$\lambda^X_Y$, $\mu^X_Y$ failure/recovery rate of y element related to X system

stakeholders on DERs with cyber-physical system (CPS) be affected in the context of reliability-risk managements and what will the economic implications be?

Published literature addresses a limited part of cyber-physical interactions with PV systems reliability, in the purview of DER integration and CPS's availability/unavailability modelling.

The paper makes several new contributions proposing an innovative mathematical framework to determine steady-state failure rates of cyber-physical systems considering availability & unavailability of cyber-physical components with varying levels of intensity (severity) of cyber-attacks. They are:

(1) A new mathematical framework is proposed to reduce assessment process complexity of cyber-physical systems in a holistic way.
(2) An algorithm is proposed by incorporating framework in (1) for the reliability assessment of a PV integrated power system with cyber-physical interactions at PV connections.
(3) Sensitivities of CPS repair times are assessed.

The paper is outlined in the following structure. Section 2 delineates on most relevant works to the research problem; Section 3 presents the newly developed homogenous Markovian reliability model of PV system elements and a model for CPS failure and repair times; Section 4 gives different case studies that show repair time related impacts and sensitivities on a power system, and finally Section 5 concludes findings of the investigation.

## 2. Related research work

Despite the fact that reliability issues of photovoltaic (PV) components have already been identified to date, the reliability analysis of PV generation elements as a unified system is lacking at a component level because of the system complexity. A great deal of previous research into PV reliability focused on power electronic element levels that evaluated inverter and aging performances [5–7]. There is little research on PV reliability evaluation where reliability of a PV system has been assessed as an entire system with very detailed components of the PV system.

A Markov chain comprehensive study of PV system reliability is proposed in [8], where three different PV systems were examined under various circuit conditions of combined component-wise. According to [8], design variations on a PV system and its component changes contribute to a different level of operation cost to operators and the impact of temperature rise on PV components reduces system reliability and increases overall PV generation cost. In view of the maximum reliability-minimum cost criterion, reliability of such a PV system should be considered not as a single unit but also as a combination of component-wise reliabilities to determine the realistic PV intermittency impacts [9]. The authors of [8] successfully evaluated combinations of PV components' state transitions and temperature effects with uncertain working conditions of PV systems on power grid performance, but the study did not incorporate cyber-physical component-related failures with PV systems that may lead to a considerable change on performance of a power system operation and repair strategies. Moreover, there is no reliability criterion demonstration of a network considering impacts of PV's and its components' repair time strategy [9], which may influence generation capacity and energy yield. This is also evident from the findings and suggestions in [10,11] which demonstrate the importance of the role of PV repair time strategy on accurate reliability-lifecycle quantification of PV systems. It is worth noting that Dhople et al. [10] implemented Markov reward model to grid-connected PV systems for analysis of lifetime energy yield and its performance. Yet, they only considered two failure strategies that are string block and inverter, which are not adequately represent failure mode considerations in terms of reliability-lifecycle to determine an accurate reliability performance index. A detailed characterization of PV system components in the context of reliability provides useful data for power system planning and repaires as well as optimizing operation cost [11]. Furthermore, the studies in [10,11] would have been more interesting if they had included cyber-physical system (CPS) as another sub-system to assess overall reliability on PV system operation & repair. Although, all the previously mentioned Refs. [5–11] cover the aspect of unified component-wise reliability of a PV system, the studies are deficient in determining the importance of the CPS effects on PV systems reliability.

Most of the studies attempted to evaluate the impacts of cyber-attacks and types on electricity networks. It was also argued that cyber-attacks on power systems could lead to damage power lines and system outages [12]; additionally, in [13], the influence of the vulnerability of two-way communications on the power systems were explored; these studies found that malicious attacks with manipulative interactions on smart meter data can bring higher energy costs to customers as well as to system operator. Another study in [14] showed that different types of cyber-physical attacks on voltage regulation schema of power grids can reduce power output of a PV system significantly. According to the impact studies, detection of cyber-physical attacks has an essential position on power grid operation. Although most works demonstrate how cyber incidents could influence a power system, no clear method was suggested for PV system integrated reliability assessment with cyber-physical interactive operations. As stated before, classical reliability studies on PV systems have taken into consideration all PV system elements, except CPSs. What we know about CPS's reliability on energy networks is largely based upon theoretical studies that investigate how various kinds of cyber-attacks considering offensive and defensive mechanisms are going to affect power system reliability [15–17]. Furthermore, there are more recent studies focused on the provision of successful and unsuccessful cyber-attacks reaching critical assets such as SCADA [15–17]. Thus, it is apparent that no adequate attempt was made to quantify the association between distributed energy resources (DERs) and cyber incidents that it is important in the pathway to integrate smart power systems with renewable energy resources. Furthermore, the knowledge of how CPS's repair time influence on power system reliability performances is vital in the smart power system design journey.

## 3. Mathematical modelling

### 3.1. Reliability modelling of PV system

Power systems broadly consist of several sub-systems that involve some devices or components linked either in series or parallel system configurations. To do robust analyses on the reliability of PV systems,