Reliability Assessment of a Power System with Cyber-Physical Interactive Operation of Photovoltaic Systems

Gunduz, Hasan; Jayaweera, Dilan

DOI:
10.1016/j.ijepes.2018.04.001

Document Version
Peer reviewed version

Citation for published version (Harvard):
Gunduz, H & Jayaweera, D 2018, 'Reliability Assessment of a Power System with Cyber-Physical Interactive Operation of Photovoltaic Systems', *International Journal of Electrical Power and Energy Systems*, vol. 101, pp. 371-384. https://doi.org/10.1016/j.ijepes.2018.04.001

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

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.

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

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
λ_{CC}, μ_{CC}	Failure/Recovery rate of Charge Controller
λ_{BB}, μ_{BB}	Failure/Recovery rate of Battery Bank
λ_{MI}, μ_{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
λ^X_Y, μ^X_Y	Failure/Recovery rate of Y element related to X 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 8,000

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. Tel.: +441214142934

E-mail Addresses: hxg461@bham.ac.uk (H. Gunduz), d.jayaweera@bham.ac.uk (D. Jayaweera).

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 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 references [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, series or parallel arrangements of system components have critical roles

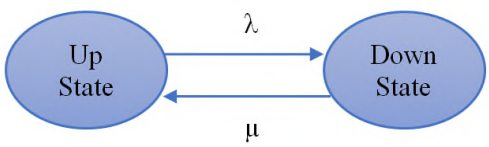


Fig. 1 State diagram of single unit Markov chain

. In relation to these criteria, equations, this section shows how to develop a generic reliability model of a PV system in connection with inverters and critical components.The system's failure and repair rates (λ_{System}, μ_{System}), availability and unavailability indices (A, U), and failure-repair state probabilities (P_f, P_r) have been developed as in **[18]**. In this section, a mathematical model and a PV system configuration are also presented that relates to the effects of PV system components as well as cyber-physical devices influence on reliability of a power system.

So as to achieve the reliability target of PV related generator systems, in general, a 2-state 1-unit Markov chain process is implemented. UP and DOWN states give fully-operational and fully non-operational PV systems respectively in **Fig. 1**. A single line block diagram of micro-inverter related PV system is given in **Fig.2-a**. The following generalized PV model is divided into three sub-divisions for overall power system reliability analysis. For this section, the first sub-division as a serially arranged string is composed of a PV panel, a micro-inverter, and a fuse. There are n-independent of parallel strings connected as series to n-independent numbers of charge controllers with battery banks, cyber-physical interactive system components, which are part of second and third sub-divisions respectively. All sub-divisions are connected to the power grid as a serially arranged system. The system balance equivalent given in **(1)** is used for reliability indices' calculations for sub-divisions. The reliability indices' formulation of string's components is given in **(2)-(5)** which are serially arranged in the first sub-division.

$$\frac{U}{A} = \frac{P_f}{P_r} = \frac{\lambda_{System}}{\mu_{System}}, \lambda_{System} = \mu_{System} \times P_f \times P_r^{-1} \quad \textbf{(1)}$$

$$P_r^{MI} = \prod_t^n \left(\frac{\mu_{Panel}^t}{\lambda_{Panel}^t + \mu_{Panel}^t}\right) \times \left(\frac{\mu_{MI}}{\lambda_{MI}+\mu_{MI}}\right) \times \left(\frac{\mu_F}{\lambda_F+\mu_F}\right) \qquad t: 1,2,3,\dots,n \quad \textbf{(2)}$$

$$P_f^{MI} = 1 - \prod_t^n \left(\frac{\mu_{Panel}^t}{\lambda_{Panel}^t + \mu_{Panel}^t}\right) \times \left(\frac{\mu_{MI}}{\lambda_{MI}+\mu_{MI}}\right) \times \left(\frac{\mu_F}{\lambda_F+\mu_F}\right) \quad t: 1,2,3,\dots,n \quad \textbf{(3)}$$

$$\lambda_{String_t}^{MI} = \sum_t^n \lambda_{Panel}^t + (\lambda_{MI} + \lambda_F) \qquad t: 1,2,3,\dots,n \quad \textbf{(4)}$$

$$\mu_{String_t}^{MI} = P_r^{MI} \times \lambda_{String_t}^{MI} \times \left(P_f^{MI}\right)^{-1} \quad \textbf{(5)}$$

The overall first sub-group reliability indices of n-independent parallel strings can be calculated by using **(6)-(9).** Along with remaining storage system's reliability rates, which are related to the second sub-division, can be calculated from **(10)-(13)**. By means of cyber physical component's failure and repair rates that are related to the third sub-division **(14),** overall 8 different states of PV system's Markov chain transition matrix can be obtained for use on reliability evaluations **Fig.2-b**. So far, this section has focused on reliability equations of PV system's first and second sub-divisions. The following section introduces how to calculate failure and repair time of cyber-physical component for the third sub-division of PV system.

$$P_{r_{String}}^{MI} = 1 - \prod_t^n \left(\frac{\lambda_{String_t}^{MI}}{\lambda_{String_t}^{MI} + \mu_{String_t}^{MI}}\right) \qquad t: 1,2,3,\dots,n \quad \textbf{(6)}$$

$$P_{f_{String}}^{MI} = \prod_t^n \left(\frac{\lambda_{String_t}^{MI}}{\lambda_{String_t}^{MI} + \mu_{String_t}^{MI}}\right) \qquad t: 1,2,3,\dots,n \quad \textbf{(7)}$$

$$\mu_{String}^{MI} = \sum_t^n \mu_{String}^{MI} \qquad t: 1,2,3,\dots,n \quad \textbf{(8)}$$

$$\lambda_{String}^{MI} = \mu_{String}^{MI} \times P_{f_{String}}^{MI} \times \left(P_{r_{String}}^{MI}\right)^{-1} \quad (9)$$

$$P_{r_{Storage}}^{MI} = \prod_{t}^{n}\left(\frac{\mu_{CC_t}}{\lambda_{CC_t}+\mu_{CC_t}} + \frac{\mu_{BB_t}}{\lambda_{BB_t}+\mu_{BB_t}}\right) \quad (10)$$

$$P_{f_{Storage}}^{MI} = 1 - \prod_{t}^{n}\left(\frac{\mu_{CC_t}}{\lambda_{CC_t}+\mu_{CC_t}} + \frac{\mu_{BB_t}}{\lambda_{BB_t}+\mu_{BB_t}}\right) \quad (11)$$

$$\mu_{Storage}^{MI} = \sum_{t}^{n} \mu_{Storage}^{t} \qquad t: 1,2,3,\dots,n \quad (12)$$

$$\lambda_{Storage}^{MI} = \mu_{Storage}^{MI} \times P_{f_{Storage}}^{MI} \times \left(P_{r_{Storage}}^{MI}\right)^{-1} \quad (13)$$

$$\lambda_{Cyber}, \qquad \mu_{Cyber} \quad (14)$$

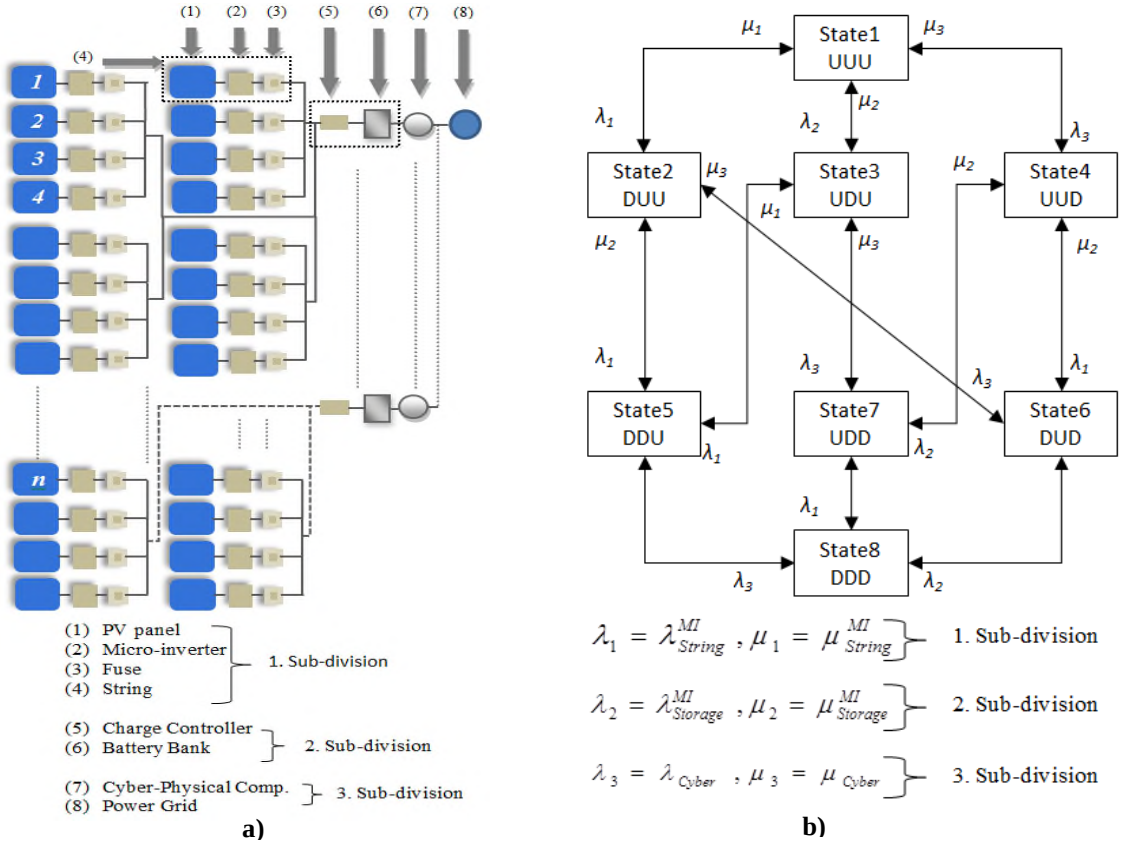


Fig.2 a) Block diagram of PV powered system with CPS

b) Probabilistic Markovian framework for the PV powered system

3.2. Reliability Modelling of Cyber-Physical System

CPS, in the context of smart power systems, is a control &-monitoring mechanism that consists of physical and virtual layers. CPS's physical layer consists of variety of actual devices, such as generators, distribution &-transmission lines and substations. The cyber layer, which is connected to virtual world, includes control &-monitor managers, energy management systems and SCADA

networks. Virtual part of the energy system is composed of CPS components and interacts with the physical part of the power system [19].

It is important to point out in view of the PV system operation &-risk assessment that not only estimation of CPS reliability indicators is a challenging task, but also cyber-attack detection because of CPS uncertain working conditions. Therefore, 2-state Markov-chain model as fully and non-operational is considered as a working principle of CPS components [20]. Poisson random numbers are used for rare event sampling in a fixed space. Previous studies that suggest not all cyber-attacks with different intensity levels can cause a failure in a power system and it is a rare event to be experienced. In addition to, Palm-Khintchine theorem [21], which is utilized reliability modelling in computer science, is justified theoretically why poisson-random numbers could be used in this study. Because of these reasons, poisson distribution is well-fitting in this concept. In order to decrease complexity of attack modelling, some assumptions are made for this study as follows:

- Cyber layer of the CPS has no partially-working principle and the conventional power system is not composed of any cyber-attack defence mechanism.
- The cyber layer of CPS's permeability in the power network is constant and memoryless.
- Number of random cyber-threats and of simulation iterations are selected as 10,000 per year.
- Random cyber-attack intensity is assumed as an arrival rate of attack to the cyber layer. Following this, comparison of the attack rate and the cyber layer of CPS's permeability determine the probability of a successful intrusion.

The main target of the framework given in **Fig. 3** is to compute availability &-unavailability indicators of CPS by means of the studies in [22, 23] and to apply Poisson distribution for successful cyber-attacks. The research in [22] aimed to evaluate NESCOR (National Electric Sector Cybersecurity Organization Resource) study group's research on generic electric sector failure scenarios. The study classified cyber-threats into three rationalized categories as follows:

- Confidentiality of a cyber-attack is defined as the probability of attacker to reach data and steals the data or information. There is no harm or damage impact on energy networks.
- The definition of integrity cyber-attack is the information changes or data manipulation /corruption in the power system. There are still no outages in power system.
- Availability cyber-attack is identified as the ones in which the system influenced is unavailable for standard working environment. The lack of availability causes the system outages.

This study is focussed on system availability problem, which can provoke the system for large outages. According to [22], unavailability in perspective of a power system is defined as large scale outages and high intensity of cyber-attack is defined as high level of power system outages. In order to calculate availability rate of CPS, the study needs to obtain a cyber-attack permeability &-intensity criterion, which can help to determine the severity level of a cyber-attack that can lead to force the system outage. The study assumes that cyber-attacks with different intensity level which are categorised confidentiality, integrity and availability attack configurations to impact on system status. If cyber-attack intensity level passes permeability-intensity limit criterion of the system cyber layer, cyber-attack intrusion into system is achieved successfully. Thus, CPS is going to be unavailable and it is associated with system contingency. The probability of permeability-intensity criterion is obtained from [22], which is 0.88 and it is used for the mathematical framework. These constants assist for investigating number of CPS outages in the specified time limit, which a year in this simulation. The framework should consider asynchronous nature and different strength levels of cyber threats. We considered that high intensity (strength) level of cyber-attack brings security failures on CPS. Within this perspective, the study can achieve a reasonable constant availability rate of CPS in the context of power systems.

Computation of availability-unavailability of CPS is illustrated as in **Fig. 3** and CPS failure-restoration indicator calculation agenda is described in following steps:

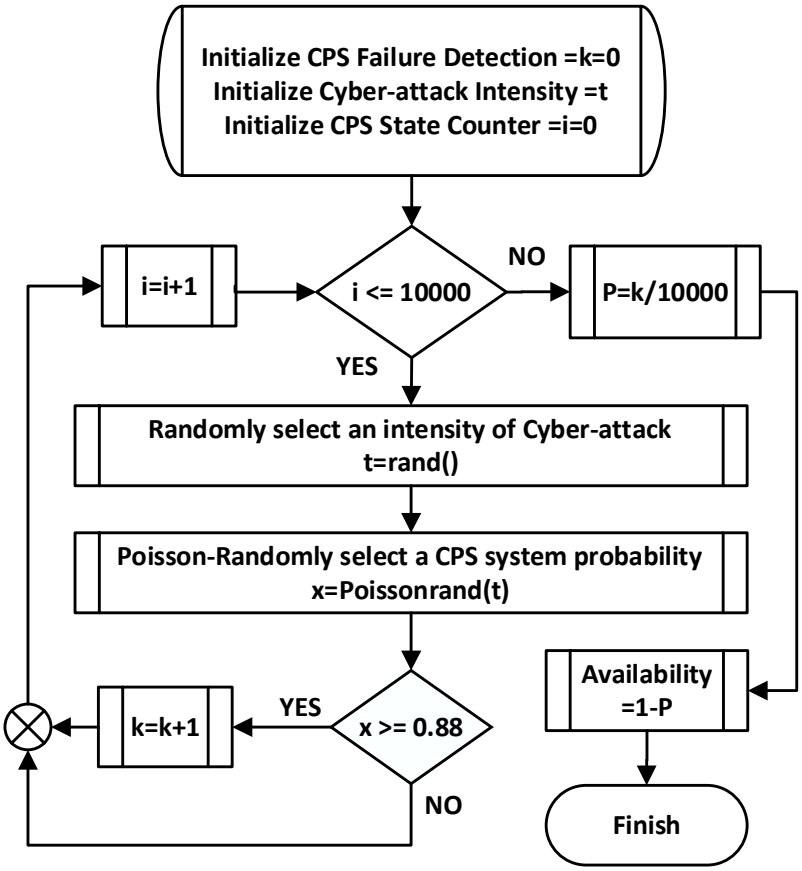


Fig. 3 Process flow diagram for availability evaluation of a cyber-physical system

1. Initialize CPS's failure detection, cyber-attack intensity rate and of the state.
2. Determine the total number of cyber-attacks in the simulation.
3. Randomly select an intensity rate of cyber-attack
4. Constitute poisson-randomly an arrival rate of attack via selected attack-intensity.
5. Check cyber-attack permeability-intensity criterion on the cyber layer and following that, raise CPS failure number only if cyber-attack permeability-intensity criterion is linked with cyber-attack intensity ratio. Cyber-attack permeability-intensity criterion determines CPS status and limits number of outage caused by cyber-attack intensity level.
6. Follow the framework until the number of cyber-attacks is fulfilled and then control with the criteria of permeability-intensity.
7. Compute CPS's availability-unavailability.
8. To do sensitivity analysis on repair-time strategy of CPS in the light of power systems, choose established one of the CPS repair-time strategies (low, medium, and high mean recovery time).
9. Afterwards, time to repair (*TTR*) **(15)** of CPS are determined as in following formula

$$\frac{1}{\mu_{Cyber}} = Time\ to\ Repair\ (TTR) \tag{15}$$

μ_{Cyber} with the unit of (/year), where, is repair rate of CPS. TTR with the unit of (hour), where, is the time to repair of CPS.

10. By the help of the below equation**(16)** [24], failure time estimation of CPS (λ_{Cyber}) dependent upon its availability is calculated as follows:

$$\lambda_{Cyber} = \frac{8760 - 8760 \times A}{TTR} \tag{16}$$

A is availability rate of CPS and λ_{Cyber} with the unit of (/year), where, is failure rate of CPS. 8760 is accepted to be a year time.

3.3. Power System Reliability Assessment Framework

The fundamental objective of reliability-based studies in a power system is to find out the system capacity limits to meet the electricity demand of consumers for a specific period. The approach adopted for reliability assessment of power system by additional incorporation of CPS availability evaluation in the standard reliability evaluation procedure steps are given below:

Step 1: Model and figure out power system's critical components related to PV systems, time series of PV power output and load demands.

Step 2: Investigate and ascertain all component failure rates of buses, lines, etc. and all previously highlighted elements of PV system.

Step 3: Compute failure-repair rates of all subordinate groups under favour of algorithm and repair-time strategy. As stated previously, Markov chain transition matrix applies with failure-recovery time of three PV system subordinate groups. After that, determine probabilities of PV system's operational and non-operational conditions.

Step 4: Randomly sampling a system state of CPS and PV system.

Step 5: Initialise power balance and consider global voltage limits during the load flow analysis.

Step 6: Implement at least 10000-iterations for each non-sequential Monte-Carlo simulation, perform optimum power flow with MATLAB-DIgSILENT integrated platform (**Fig. 4**) and calculate Expected Demand Not Supplied (*EDNS*) using [9, 25].

$$EDNS = \sum_{i \in S_i} L_i \times p_i \tag{17}$$

EDNS with the unit of GW, where, S_i is system state i; L_i is load curtailment in system state i; p_i is the system state probability.

Step 7: In final stage, universally accepted reliability index that is Expected Energy Not Supplied (*EENS*) **(18)**, is computed with *EDNS* following formula [18]:

$$EENS = \sum_{i \in S_i} L_i \times p_i \times 8760 = EDNS \times 8760 \tag{18}$$

The *EENS* is with the unit of GWh/year.

As shown in **Fig. 4,** there are two parts in the MATLAB-DIgSILENT integration platform. In the first part, the MATLAB is used to calculate availability and unavailability rates of cyber-physical system (CPS) interactive platform in order to determine its failure and repair.

According to the selected repair-time strategy of the CPS, the availability of CPS interactive platform is calculated using the procedure given in **Fig. 3**. This data is used to calculate the failure rate of the CPS interactive platform. Next, the repair-time strategy and the CPS failure rate are fed into the eight-state Markovian model together with the failure rates and the repair times of PV sub-system components. The entire intact system gives the availability and the unavailability of the PV power generation and the state-probabilities of the composite PV system in the CPS intact system model. The elements in the 8x1 state-transitional matrix give the eight-state operational and non-operational statuses of the PV power generating system with CPS operation. The data in the 8x1 state matrix is then fed into the PV power generation subroutine in DIgSILENT software [25].

In the second part of the procedure in **Fig. 4**, the data of composite 8-state PV power generation probabilities that were calculated by Markov chain model in MATLAB is fed into multi-state stochastic power generation model in DIgSILENT (StoGen). It is an element in each PV power generator (ElmGenstat). The resulting data of 8-state PV system probabilities and availabilities in StoGen are fed to Monte Carlo Simulation platform through optimal power flow routine to estimate EDNS and then EENS of scenarios.

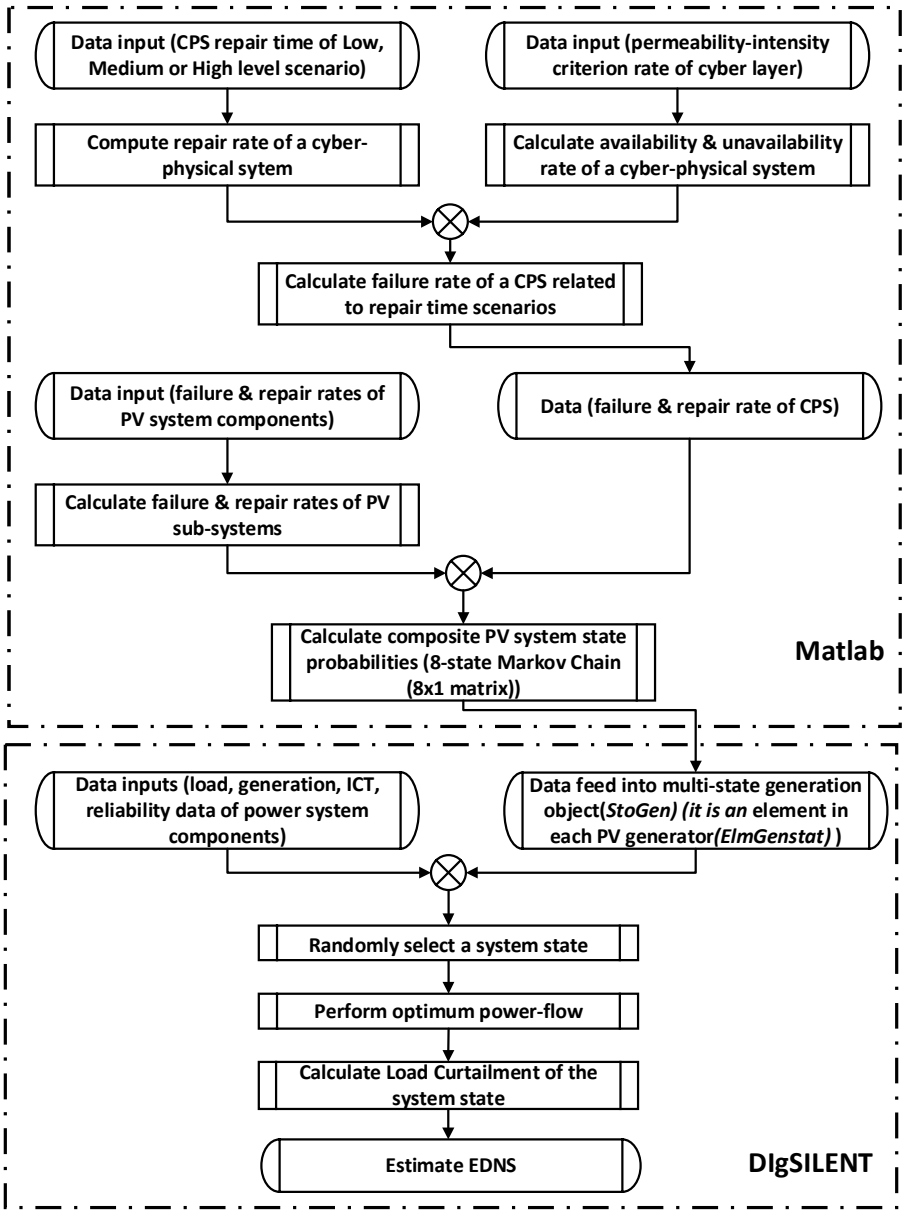


Fig. 4 Reliability evaluation framework in the MATLAB-DIgSILENT integrated platform

4. Case Studies and Results Analysis

4.1. Reliability Test System Topology and Reliability Data

4.1.1. ICT Extension with Busbar Protection for Reliability Assessment

Cyber part of energy networks in a power system is involved as secondary side terminology in power system analysis up to now. With increased carbon-emission transitions in energy sector and their interactions with information and communication technologies (ICT) in a smart grid environment, power system research also covers test systems with ICT features for realistic power system evaluations. There is a recently published benchmark study [26], which gives an example of a protection configuration of substation extension with intra and interdependent ICT elements. In this study, extended versions of RBTS and IEEE RTS79 are incorporated while considering the protection system IEC 61850 standard in substations. References [26-28] provide the detail of the architecture of ICT components in the substation. The architecture of the protection based substation is considers as a design standard for power systems [28]. **Fig. 5** shows the detailed architecture at Bus 3 in the IEEE RTS79 system.

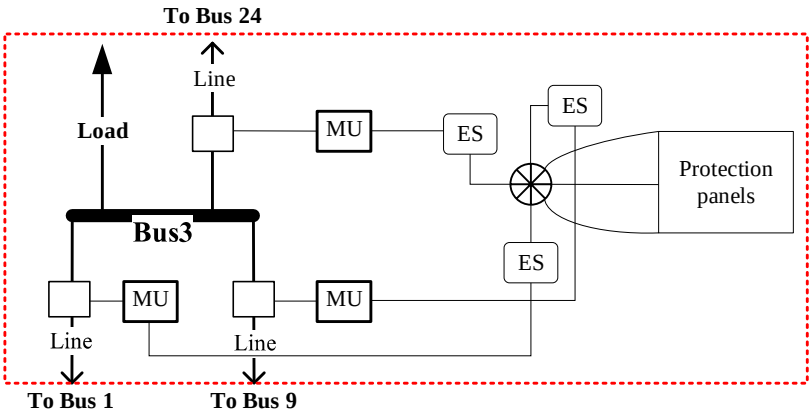


Fig. 5 An example of Cyber part extension of Bus 3 in IEEE RTS79

Due to the natural complexity and variety of ICT components, it is very crucial to take into account cyber-features in a power system evaluation. Therefore, this study is only extended to bus 3, 4, 8, 9, 10 and 13 of IEEE RTS79 with an interdependent cyber part that consists of a merging unit (MU), ethernet switch (ES) and line protection panel. These components in each power line are connected to each other as a series. Extended and traditional version of the transmission reliability benchmark system [26] are implemented in other case studies. An example of ICT element extension is shown in **Fig. 5.** The topology for traditional transmission system IEEE RTS79 and IEEE RTS79 extended version with ICT substations are given in **Fig. 6.** The traditional test system has 24 buses and 32 conventional generators with the system peak active power load of 2850 MW. The parameters for reliability analysis were obtained from [29].

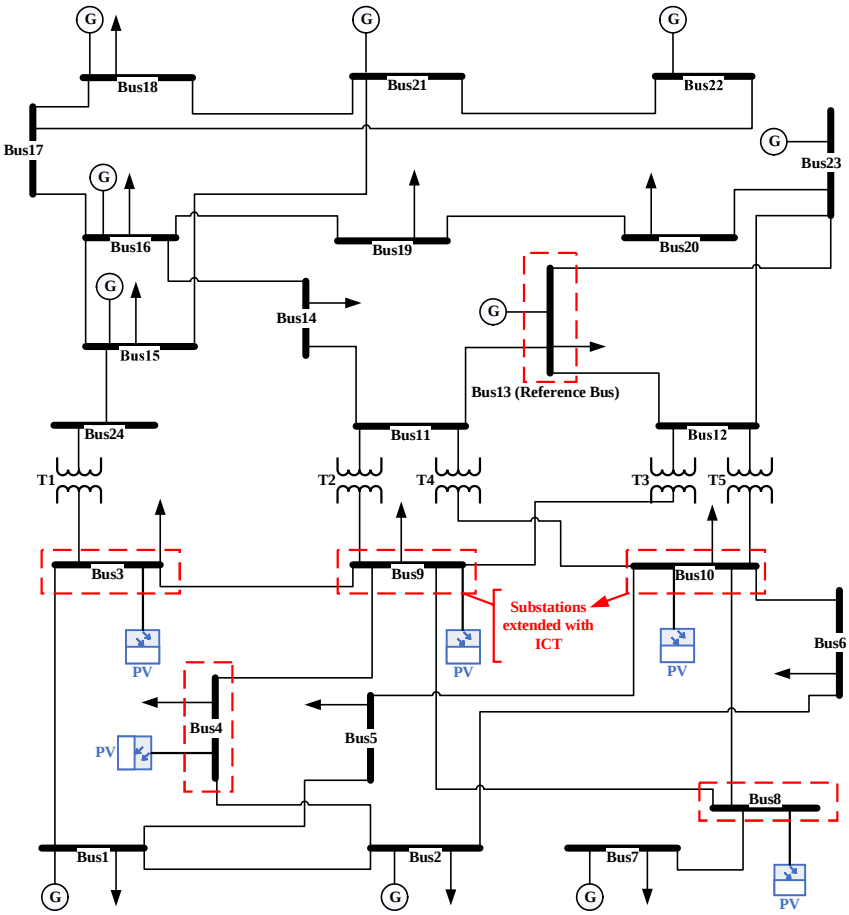


Fig. 6 Schematic diagram of IEEE RTS79 with PV systems and ICT extended version

System topology is extended to add PV systems as either centralised or decentralised. Bus 9 is specifically used for centralised PV generator integration due to exhibiting specific characters at the location. Additionally, bus 3,4,8,9 and 10 are utilised as decentralised integration nodes of PV generators. Nominal capacity of a PV connection at a consumer was assumed as 4 kW. Aggregated number of consumers at the substations is 949,994. The parameters of the PV system are extracted from [30, 31] for case study.

4.1.2. The RBTS extended with ICT configurations, PV system and CPS Reliability Data

The Roy Billinton Test System (RBTS) is used for reliability analysis in this study considered as a distribution system. This test system consists of 9 transmission lines, 6 main substations and 230 kV, 138 kV, 33 kV, 11 kV and 400 V terminals are identified as voltage levels [32]. The nominal generation capacity of RBTS is 240 MW with 11 generators and the nominal peak load capacity is 185 MW. System topology is extended to add PV systems as either centralised or decentralised and ICT components in specific substations. Bus 3 is specifically used for centralised PV generator integration in RBTS. Additionally, bus 3, 4, 5 and 6 are utilised as decentralised integration nodes of PV generators. Nominal capacity of a PV connection at a consumer was assumed as 4 kW. PV systems are connected to 11 kV voltage level. Aggregated number of consumers at the substations is 18,308. The parameters of the PV system are extracted from [18, 30-32] the study. ICT extended version substation of RBTS is developed similar to as IEEE RTS79 ICT extension. ICT extension of substation is detailed in **section 4.1.1** and demonstrated in **Fig. 5.** The same strategy is implemented into 6 buses of RBTS. The single line diagram of RBTS ICT extended version with PV generation is shown in **Fig. 7.**

The PV system component and reliability data are given in **Table 1** for both reliability test systems. As part the of reliability calculation of CPS, repair time of CPS is not available for reliability analysis. However, we have considered the recently published scientific report that gives estimated recovery time of business companies after most disruptive breach in the context of cyber security. According the report, 57% of firms affected by cyber-attack recovered within less than 24 hours [33] and remaining firms recovery time spans from weeks to months. To calculate CPS's failure rate, our study considered repair time of CPS as 15, 30 and 60 hours. In terms of low to high level harmful levels of cyber-attacks on a power grid, repair-time strategies are designed accordingly. Error! Reference source not found. **Table 1** also gives repair-time strategies of CPS considering low, medium and high-level. The reliability data of components was used for the sensitivity analysis with CPS's repair-time strategies and following that, failure rate computation of CPS is determined using (16) after computing the availability of CPS.

Table 1. Reliability data for PV system [30, 31], ICT components[26] and CPS repair-time strategies

PV System and ICT Components	Failure rate	Repair rate
PV panel	1.14×10^{-6}	0.0209 (48h)
Micro-inverter	0.05	0.05(20h)
Charge-controller	0.125	0.1(10h)
Battery bank	0.00702	0.0825(12.11h)
Fuse	0.00137	0.05(20h)
Merging unit	0.02	8h
Ethernet switch	0.01	8h
Protection panel	0.02	8h
Repair Strategy	Failure rate	Repair rate
High Repair Time	0.019	0.016 (60h)
Medium Repair Time	0.0097	0.033 (30h)
Low Repair Time	0.0048	0.066 (15h)

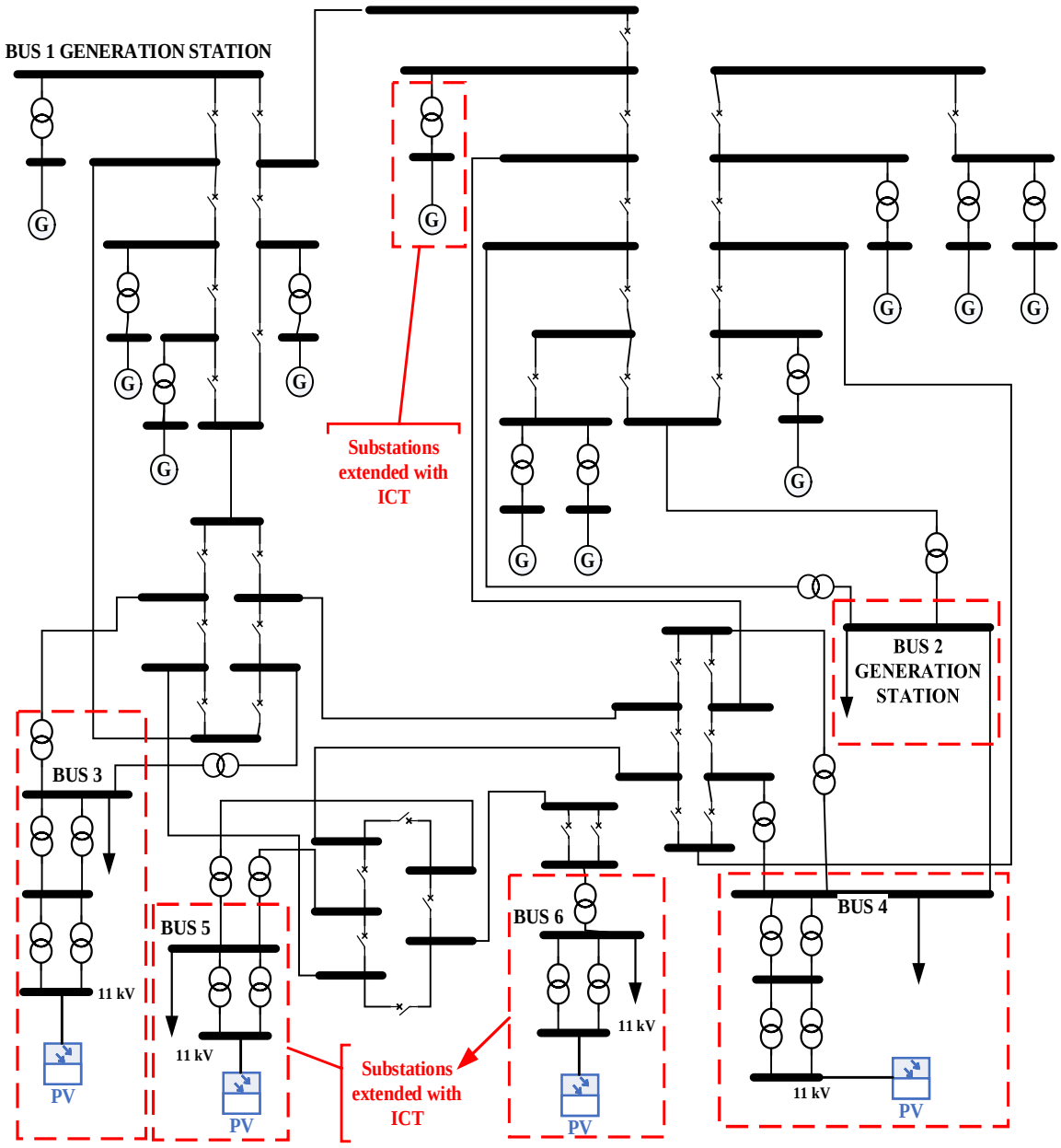


Fig. 7 Schematic diagram of RBTS with PV systems and ICT extended version

4.2. Case Study 1: High Level PV Penetration in IEEE RTS79

The aim of this study is to demonstrate impacts of CPS's repair time strategy on the power system reliability when the PV generation capacity level increases in the power grid. In addition, power system reliability analysis is considered with ICT protection components extended and original version of IEEE RTS79 in context of centralised and decentralised PV penetrations. We compared EENS results of traditional transmission test system with ICT extended version of it.

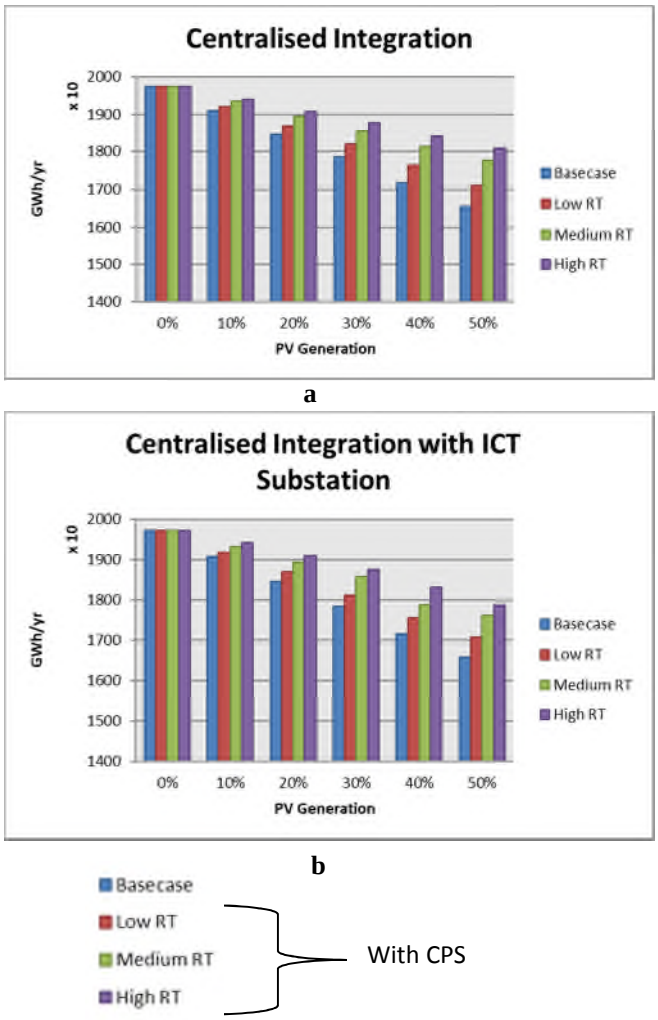


Fig. 8 EENS for the centralised PV and centralised PV integration extended with ICT feature

(a) Centralised integration of PV in IEEE RTS79

(b) Centralised integration of PV in IEEE RTS79 extended with ICT feature

The simulation for this study is performed on a computer with a 2.4 GHz processor and processed time for IEEE RTS79 with centralised and decentralised PV integration is around 10 seconds. IEEE RTS79 extended version with cyber-induced terminals reaches almost 12 seconds because of additional ICT protection components. PV system penetration level is varied from load base case (0%) level to 50% of the base case level. **Fig. 8** and **Fig. 9** show that an increment in PV generation reduces the EENS index of the power grid because of the high integration level of the PV generation. In all (centralised, centralised with ICT, decentralised and decentralised with ICT) cases, it can be observed that the CPS has an adverse effect on the EENS. With an increase in PV generation with cyber-physical system, EENS abruptly increases. Although there is essentially an increase between repair time rates, the EENS of all repair times of PV system with CPS is higher than the PV system base case. Results show that when PV generation is increased in the grid, EENS of the system is decreased linearly in all cases. Especially, in case of 40% and 50% PV generation level, there is a slight increment of EENS, compared to the cases of 10%, 20%, and 30%. The reason of this disparity of EENS increase is due to different failure-repair rates of the cyber-physical system, which changes availability-unavailability ratio of PV generation on the power network systematically. There is no considerable difference between all other cases. However, when the PV penetration increases above 30%, CPS repair time is at the lowest point in order to limit EENS. Economically, it may be more favourable to select low repair time strategy to minimize impact of labour cost during the repair-time. According to EENS values, the centralised system is slightly more reliable than the decentralised

system even when we introduce CPS because of intact operation of CPS compared with decentralised operation.

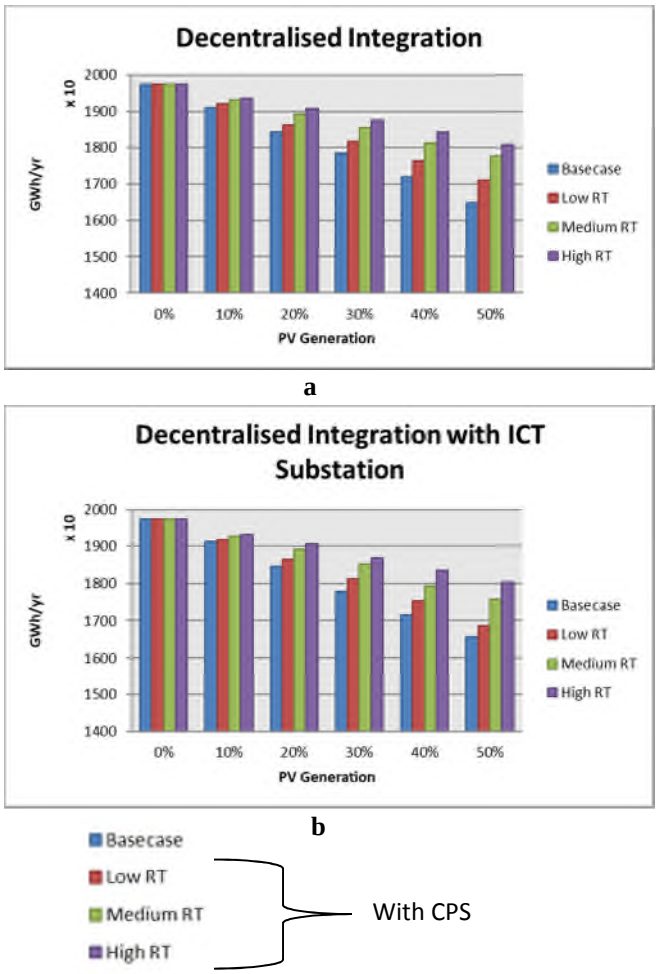


Fig. 9 EENS for the decentralised PV and decentralised PV integration extended with ICT

(a) Decentralised integration of PV in IEEE RTS79

(b) Decentralised integration of PV in IEEE RTS79 extended with ICT

After specified substations extended with ICT protection components, there are slight decreases in EENS when system is penetrated with a centralised and decentralised PV systems. The main EENS disparity can be observed in **Fig. 8-b** and **Fig. 9-b.** ICT protection elements changes EENS between 0.1% and 1.4 % compared traditional transmission system in both distributed and centralised cases. When PV penetration level reaches up to 40 % and 50 % of base case with medium and high repair time of CPS categories, the impact of ICT protection components on the system reliability can be observed on test system clearly.

4.3. Case Study 2: Comparison of PV and Synchronous Generator for IEEE RTS79

The aim of this study is to understand system reaction and sensitivity of CPS repair time strategies when the PV systems are integrated, instead of conventional generation. In this case study, a strategy was adopted with a 5 MW PV generation capacity increase; a reduction of 5 MW conventional generations on slack bus (Bus13) of IEEE RTS79 was incurred. This approach is applied into centralised &- decentralised generation with and without ICT protection components up to 25 MW PV generations in order to see impacts on EENS. It can be observed from **Fig. 10-a** and **Fig. 11-a** that an increase in PV generation reduces EENS of the power grid in the case of Low RT, Medium RT and Base case. The system becomes more reliable compared to the base case of the centralised system **(Fig. 10-a).**

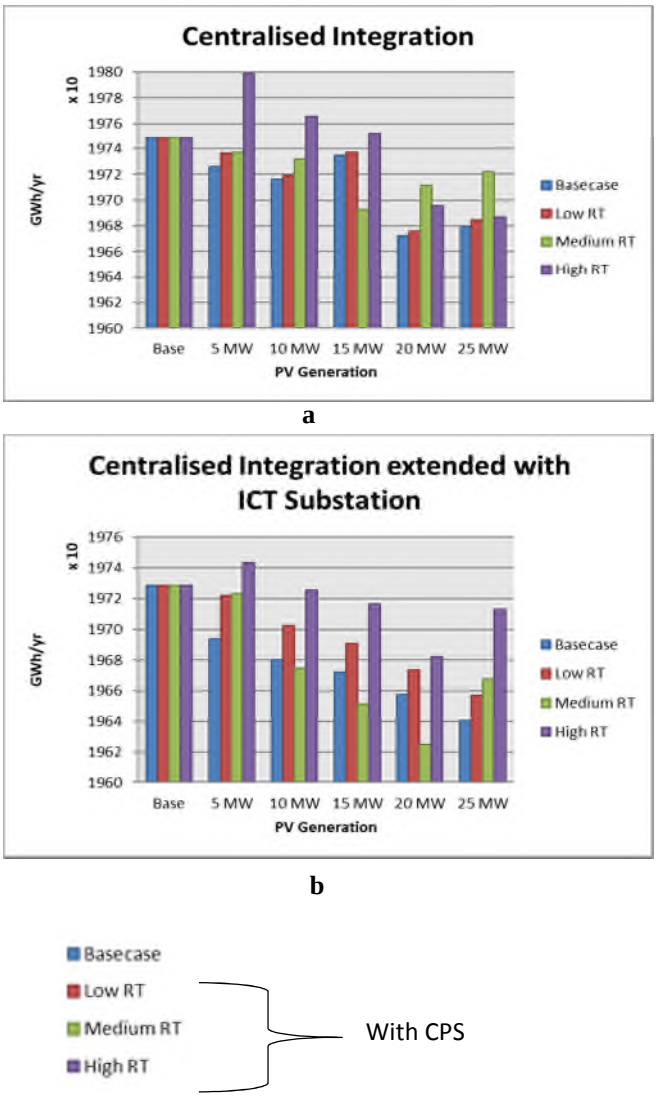


Fig. 10 EENS variation in centralised PV with different topological features

(a) Centralised PV integration in IEEE RTS79

(b) Centralised PV integration in IEEE RTS79 extended with ICT feature

Also, sudden changes are more eminent with an increase in decentralized PV integration (**Fig. 11-a).** A unique change developed in this case is the increase in high repair time even at 5MW PV generation. In spite of the fact that mean time failure rate of synchronous generator is less than PV generator failure rate, deployment of PV generator at slack bus reduces EENS steadily. It does not necessarily mean that PV system is more reliable than synchronous generator. Apparently decrease in EENS in this case can be a result of either the system topology and location of the deployment of PV or intermittency in the power generation. The reason for the sudden changes in the PV system recovery times on EENS is the impact of PV intermittency features on generation output as well as the availability of all PV systems and the PV system location in the transmission system. This required further investigation to find out the root cause of the sudden disparities in system reliability with different CPS repair time strategies. Following this, two case studies (**section 4.4 and 4.5)** were carried out focusing on the network topology impacts on EENS in parallel with contingency analysis.

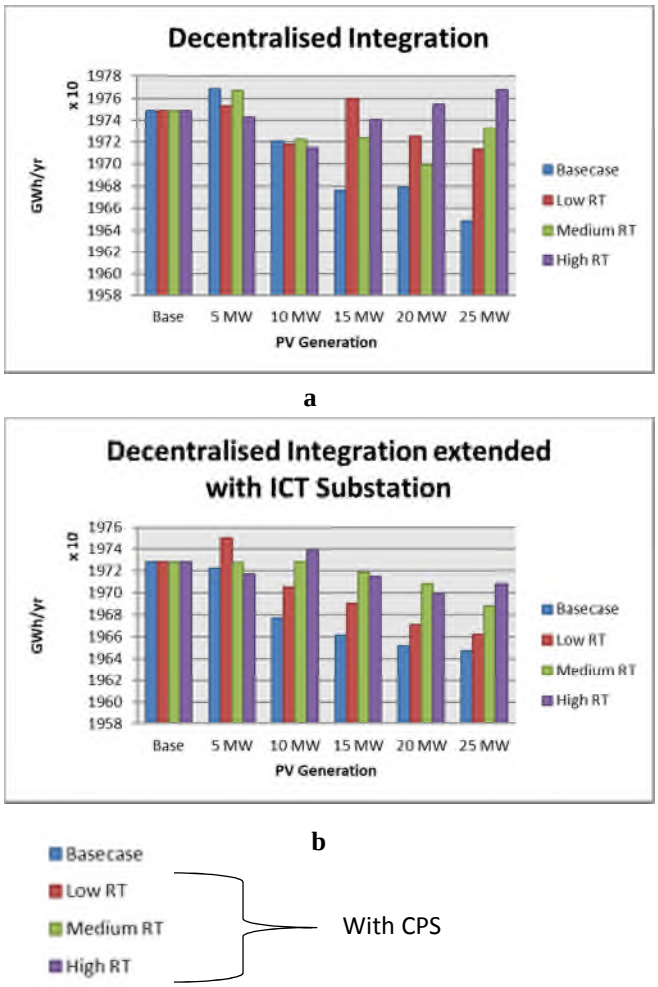


Fig. 11 EENS variation in decentralised PV capacities with different topology features

(a) Decentralised PV in IEEE RTS79

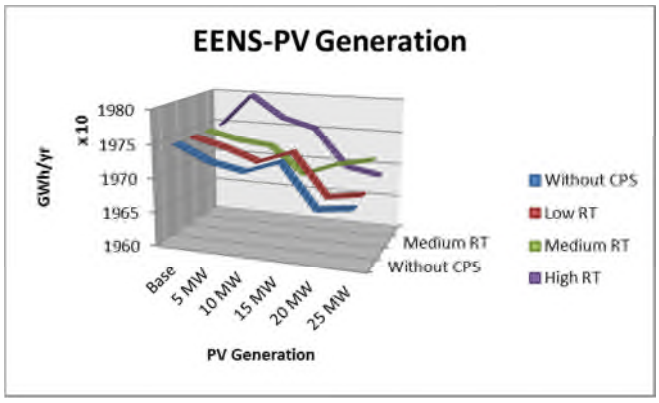
(b) Decentralised PV in IEEE RTS79 extended with ICT feature

In addition, distributed and centralised PV integration in IEEE RTS extended version with ICT protection components are compared with original IEEE RTS79 version. The results show that ICT protection system is influential for reliability improvement in a power system. It can reduce EENS significantly, effecting time in high level during the high and medium repair-time strategies of CPS. In almost all the cases, ICT protection extension has a positive influence on the system reliability improvement leading to reduce EENS between 0.1 % and 0.5 % compared with the original test system model; except 25 MW centralised PV integration considering high repair time strategy (in **Fig. 10).** Due to different buses and levels of PV penetration into the power system, impact of ICT component integration on substations varies randomly. After increasing penetration of PV generators into the system up to 25 MW, the system reliability reduces especially considering high and medium repair time strategies of CPS. It can be seen in **Fig. 10** and **Fig. 11** that between 20 and 25 MW PV generation capacity level might be held threshold point for this test system in perspective of CPS.

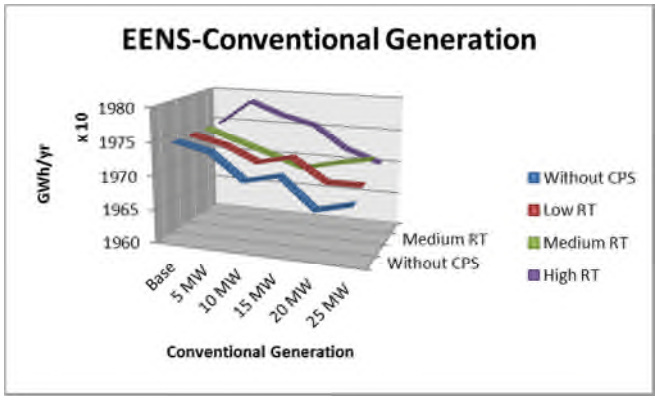
4.4. Case Study 3: Effect of Power Network Topology on System Reliability in IEEE RTS79

This case study investigates the root causes of unexpected EENS variations of PV systems observed in the case study 1 and 2. Instead of connecting PV generator on terminal 9, a conventional generator of the same generation capacity was connected. It is worth mentioning in this study that an increase on Bus 9 will remove equivalent generation capacity from the slack bus generator. If the results are similar to the PV generator, then it will reflect that the variations of EENS results were due to the power network topology. If the results are different, the EENS variation is due to PV

intermittency. In order to analyse the impact on EENS index by PV intermittency and power network topology, the conventional generator has been integrated into the network at Bus 9. Conventional generation capacity varies from 0 MW to 25 MW as done in case study 2 for PV generators. The results of this case study are demonstrated in **Fig. 12 (a), (b).** As is evident from **Fig. 12,** the EENS results of four CPS's repair time strategies with different generation capacities in the case of conventional generation was almost similar to PV generation.



a



b

Fig. 12 Comparison of EENS changes with different generation technologies on Bus 9

The small variations between both cases can be associated to the intermittency of the PV system output. Therefore, the sudden changes on EENS in case study 2 are influenced by PV system location. Because of PV intermittency, EENS changes between 0.008% - 1.2%, compared to base case. The highest EENS changes between PV and conventional generator 20 MW generation capacity with high repair time strategy of cyber-physical system (CPS) (1.2%). Also, 20 MW generation capacities with medium repair time is the most feasible PV integration for this network considering the cloudy conditions. This means the 20 MW PV-generation has least intermittency impact on the EENS in comparison to the base case EENS (0.008%) for Bus 9. Secondly, another notable observation is that peak values of EENS of PV generator are higher than the conventional generator in all repair time strategies.

4.5. Case Study 4: Contingency Analysis in IEEE RTS79

The general principle of transmission network planning is to ensure safe, secure, reliable and economically beneficial energy delivery to costumers in the future. Integration of new generation technology is one of the essential objectives for transmission operators in perspective of power system repaires and operations.

Table 2 Contingency analysis for critical components

	Centralised Integration	**Decentralised Integration**
Vulnerable Component	Bus 6	Bus 6
PV Generation	Maximum voltages (p.u)	Maximum voltages (p.u)
5 MW	1.012	1.012
10 MW	1.021	1.047
14 MW	1.043	1.049
15 MW	1.045	1.053
20 MW	1.048	1.057
24 MW	1.049	1.058
25 MW	1.050	1.058
Vulnerable Component	Transformer 3	Transformer 3
PV Generation	Maximum Loading (%)	Maximum Loading (%)
5 MW	98	97.5
10 MW	96.5	96.1
15 MW	95	94.8
20 MW	93.6	94.6
25 MW	92.1	93.7
Vulnerable Component	Transformer 5	Transformer 5
PV Generation	Maximum Loading (%)	Maximum Loading (%)
5 MW	95.4	95.6
10 MW	94.5	94.7
15 MW	93.6	93.7
20 MW	92.7	92.7
25 MW	91.8	91.7
Vulnerable Component	Transformer 4	Transformer 4
PV Generation	Maximum Loading (%)	Maximum Loading (%)
5 MW	87.9	87.5
10 MW	87.8	87
15 MW	87.6	86.6
20 MW	87.5	85.4
25 MW	87.4	84.7

To keep system performance in operation and planning standards, operators determine reliability criteria for high to low probable contingencies that has an impact on system security. Therefore, involvement of PV technology's characteristics might bring extra expenses and change security margin limits of the network [34]. The objective of this study is to examine the contingency analysis for PV system integrations on IEEE RTS79 bus system and to find out what the PV integration secure limit of the system is in the context of centralised and decentralised integration. To investigate the performance of the system in the context of voltage and loading security, single and multiple contingencies have been implemented. According to the contingency assessment, bus 6 that is connected to bus 10, transformer 3 (between bus 9 and 12), transformer 4 (between bus 10 and 11) and transformer 5 (between bus 10 and 12) are found to be as critical components for PV integration on the network. Bus 6 is selected for demonstration because it is the most violated terminal when considering centralised and decentralised integration of PV systems. It can be clearly seen in **Table 2** that the highest voltage violations arise after 24 MW and 14 MW for centralised and de-centralised PV integration accordingly. Also, there is a load violation which represents how the system is under

high risk of cascade collapse, with PV powered integrations increases. Moreover, transformers (3, 4 and 5) need to be taken into consideration of future transmission system repairs & expansion schemes by operators, especially transformer 3 in this power system. It is still overloaded (92.1 % and 93.7 %) in both integration methods while the PV integration capacity reaches up to 25 MW.

4.6. Case Study 5: High Level PV Penetration in RBTS

This case study is to show impacts of CPS's repair time strategy on the power system reliability when the PV generation capacity level increases in the distribution test system.

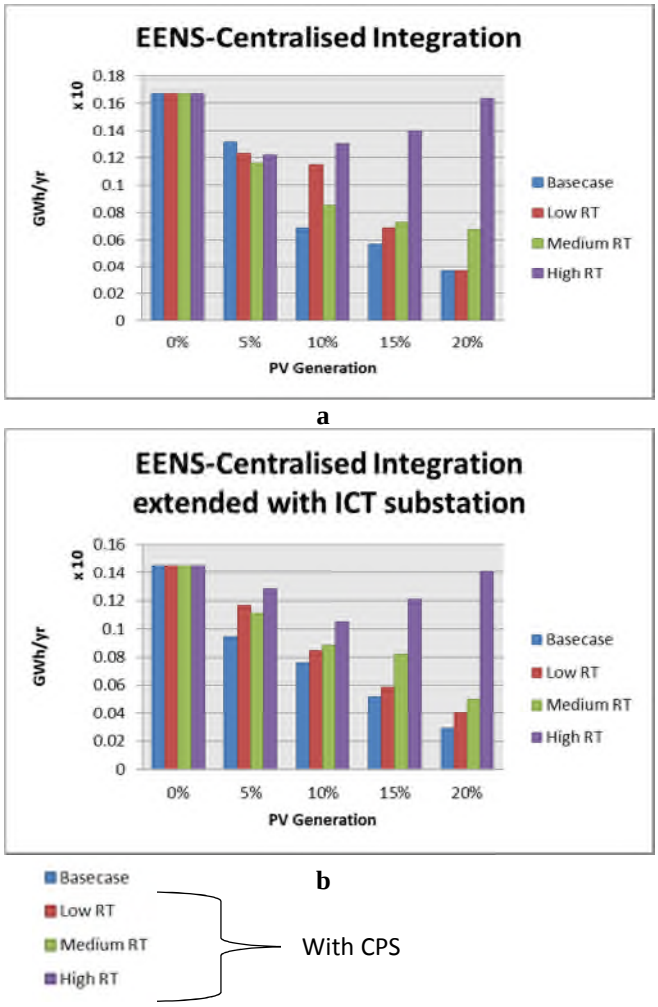


Fig. 13 EENS for centralised PV and centralised PV integration extended with ICT feature in RBTS

(a) Centralised integration of in RBTS

(b) Centralised integration of PV in RBTS extended with ICT feature

One could expect that the behaviour of a power distribution system should be different than a power transmission system due to the complexity levels and details among them. Power system reliability evaluation is considered with ICT protection components extended and original versions of the RBTS in context of centralised and decentralised PV penetrations. PV system penetration level is increased from base case load case (0%) level to 20% of the base case load level. **Fig. 13** and **Fig. 14** show that an increase in PV generation reduces the EENS of the power grid compared to base case level because of the high integration level of the PV generation. In all (centralised, centralised with ICT, decentralised and decentralised with ICT) cases, CPS has a backlash on the system reliability.

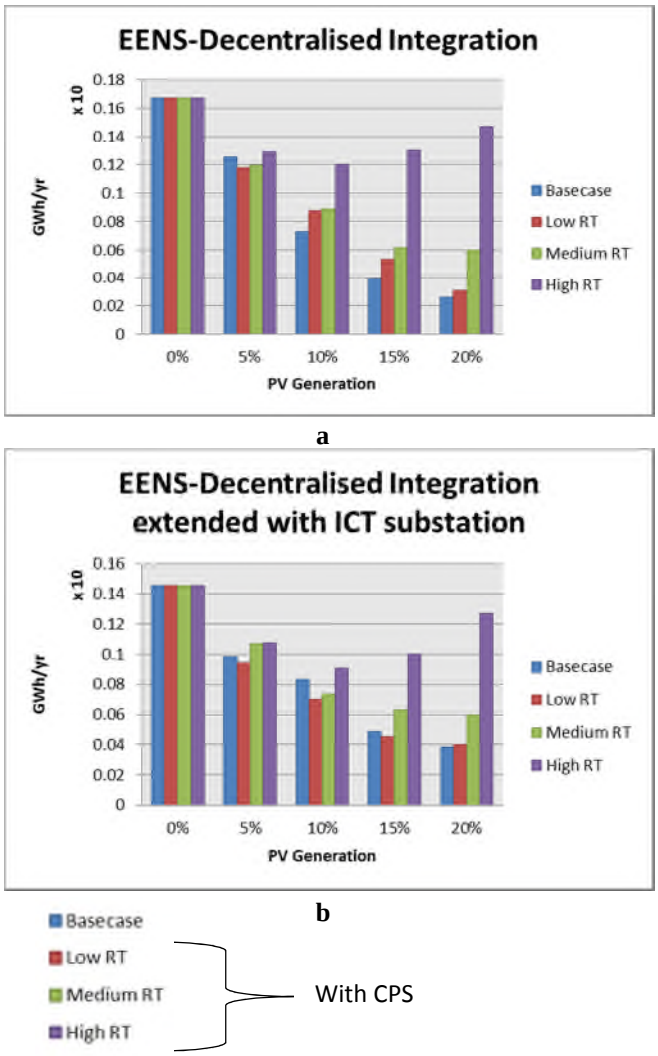


Fig. 14 EENS for decentralised PV and decentralised PV integration extended with ICT feature in RBTS

(a) Decentralised integration of PV systems in RBTS

(b) Decentralised integration of PV system results in RBTS extended with ICT

With an increase in PV generation with CPS, EENS varies suddenly. Compared to the previous reliability assessment in case study 1 what could be differently seen in this case study is that EENS of the RBTS is not rising steadily with CPS repair-time strategies. One of the reasons might be is that the RBTS is much smaller system than IEEE RTS79. The EENS changes in small system can easily be observed compared to large power system. PV systems integration with low and medium repair time of CPS act adversely affected for increment of generation in **Fig. 13-a** and **Fig. 14-a.** However, in case of high repair time, EENS increases subsequently. Although the increment of PV capacity level reaches 20% of load capacity level, the increment of EENS with high repair time strategy reaches almost base case levels. **Fig. 13-b** and **Fig. 14-b** show EENS changes on different centralised and decentralised PV penetration levels with ICT extended version of the RBTS. The major similarity in both figures is that ICT protection elements affected the system reliability in a positive way even though there is a CPS' effect. ICT protection elements with RBTS improve EENS between 13% and 25% level compared to conventional RBTS. Simulation processing time for the RBTS with centralised and decentralised PV integration varies between 10 and 15 seconds with added ICT protection-induced terminals.

4.7. Case Study 6: Comparison of PV and Conventional Generator for RBTS

The case study is aimed at PV system impact assessments with CPS on a power system. Any increase in PV power generation is reduced from the conventional power generation at Bus 1 in the

RBTS. The approach is tested through centralised and decentralised connections of PV systems with ICT protection schemes. Study assessed PV power generation capacity up to 40MW in the intervals of 10MW. Centralised and decentralised penetrations of PV systems are considered at substation 3 and (3, 4, 5, and 6) respectively; the case study topology is given in **Fig. 7.** The bar charts in **Fig. 15** and **Fig. 16** show how PV generation affects the system reliability in all cases. Results suggest that none of the case deliver EENS greater than the level of EENS in the base case.

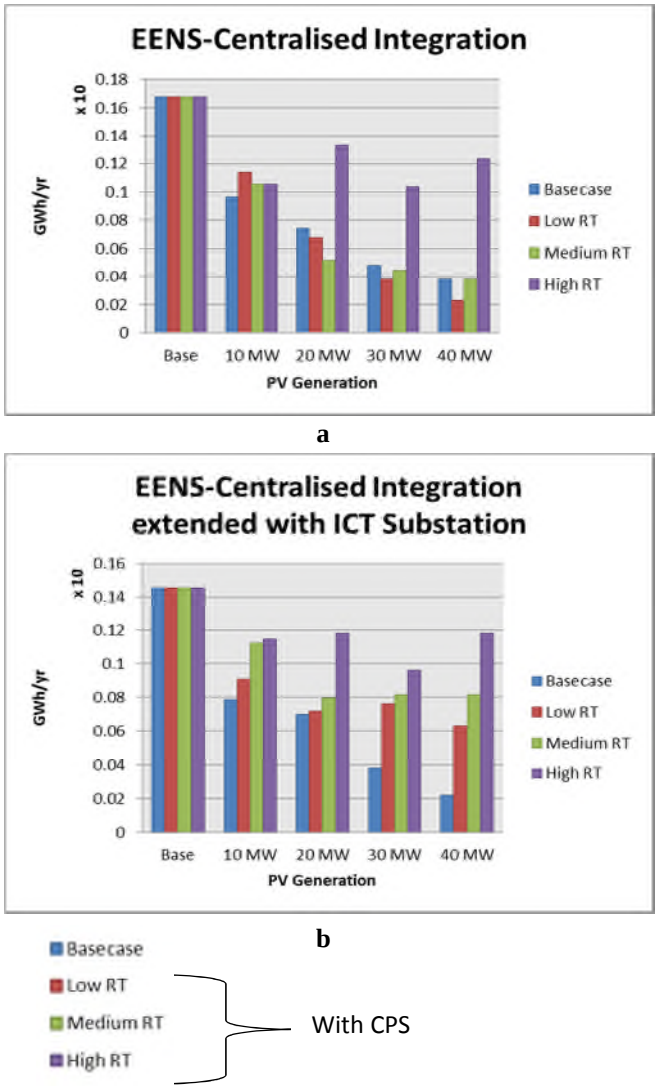


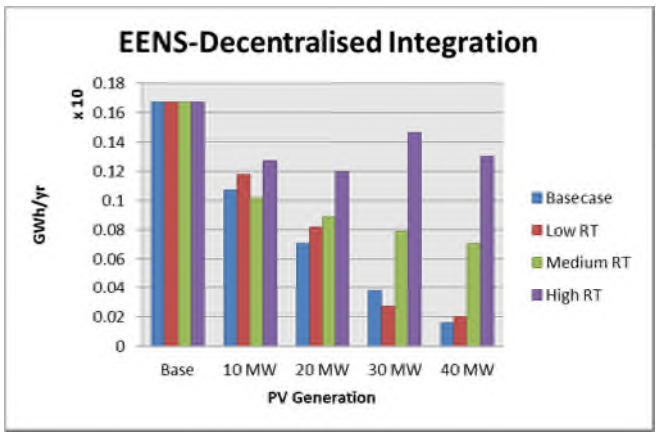
Fig. 15 EENS variation in conventional power generation and PV

(a) Centralised PV integration in RBTS

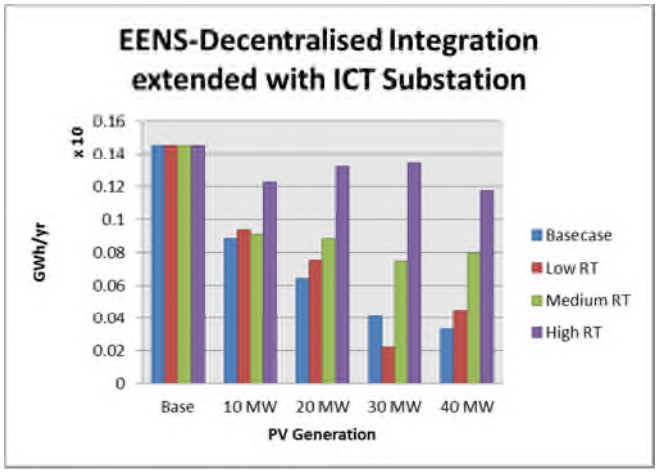
(b) Centralised PV integration in RBTS extended with ICT

The signature of EENS in the power transmission system given in case study 2 follows a different shape compared with the shape originated in **Fig. 15** and **Fig. 16.** In all repair-time scenarios, an overall downward trend in EENS can be observed from the base case to every step-increase in the PV power generation capacity, as seen in **Fig. 15-a** and **Fig. 16-a**. However, high repair-time scenarios do not necessarily conform to the downwards trend. It shows a rather a fluctuating behaviour for both centralised (**Fig. 15-a)** and distributed PV penetrations (**Fig. 16-a)** with CPS, from 10 MW to 40 MW of PV power generation. The behaviour of the high repair time scenario is due to the PV system location and loading conditions. In case study 2, the unexpected EENS variations with PV systems in the power transmission system were due to the location of the PV system. The RBTS also follows in a similar pattern when PV system penetration levels vary between generation bus (bus 1) and load buses

(3, 4, 5, and 6). This is the main reason for fluctuating EENS at high repair time scenario with centralised and decentralised penetration. Despite the distinctive behaviour of high repair-time scenarios, the overall EENS is still lower than base case scenario. Furthermore, a comparative analysis of **Fig. 15-a** and **Fig. 16-a** show that in the case of decentralized integration of PV, the improvement in reliability of the power system slightly outperforms the improvements made in the centralized integration.



a



b

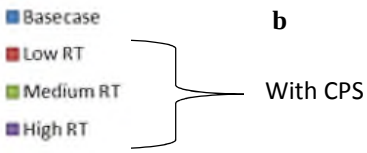


Fig. 16 EENS effects for the variation of conventional power generation and PV capacities

(a) Decentralised integration PV in RBTS

(b) Decentralised integration of PV in RBTS extended with ICT

5. Conclusion

The paper presents an innovative stochastic modelling framework for the reliability assessment of a PV integrated power system with CPS component interactions, incorporating non-sequential Monte-Carlo simulation. A part of the algorithm estimates availability and unavailability of the cyber-physical interactions at PV nodes and processed through homogeneous Markov chain. The complete approach reduces the complexity of the assessment process, reduces the processing time of the simulation, and provides an innovative pathway to assess system reliability in a holistic way.

Performed case studies suggest that impacts on PV system integration on power systems and variable threats were inconsistent against the penetration levels of PV generation. Topology of the PV system is much more influential on the impacts compared with the level of intermittency of PV power generation. The cyber-attacks propagation can be limited at centralised connection although the benefit of utilising decentralise integration of PVs are high compared with centralised integration. Thus, the high penetration of PVs can be constrained more if the power system operation incorporates internet of things environment with cyber-network operation compared with the traditional operating practices.

Proposed hybrid model can also be used in a vulnerability assessment in a power system with interactive intermittent distributed generation.

References

[1] IEA-PVPS, "IEA-PVPS Annual Report-2015 " 13/05/2016 2015.

[2] R. J. Campbell, "Cybersecurity Issues for the Bulk Power System," Congressional Research Service2015.

[3] EIA. (2017, 02/02/2018). *"How many smart meters are installed in the United States, and who has them?"*. Available: https://www.eia.gov/tools/faqs/faq.php?id=108&t=3

[4] MIT, "Utility of The Future," MIT Energy Initiative2016.

[5] R. Alonso, E. Roman, A. Sanz, V. E. Mart, S. nez, and P. Ibanez, "Analysis of Inverter-Voltage Influence on Distributed MPPT Architecture Performance," *IEEE Transactions on Industrial Electronics,* vol. 59, pp. 3900-3907, 2012.

[6] G. Petrone, G. Spagnuolo, R. Teodorescu, M. Veerachary, and M. Vitelli, "Reliability Issues in Photovoltaic Power Processing Systems," *IEEE Transactions on Industrial Electronics,* vol. 55, pp. 2569-2580, 2008.

[7] V. Smet, F. Forest, J. J. Huselstein, F. Richardeau, Z. Khatir, S. Lefebvre, *et al.*, "Ageing and Failure Modes of IGBT Modules in High-Temperature Power Cycling," *IEEE Transactions on Industrial Electronics,* vol. 58, pp. 4931-4941, 2011.

[8] M. Piri, M. Niroomand, and R.-A. Hooshmand, "A comprehensive reliability assessment of residential photovoltaic systems," *Journal of Renewable and Sustainable Energy,* vol. 7, p. 053116, 2015.

[9] Z. Esau and D. Jayaweera, "Reliability assessment in active distribution networks with detailed effects of PV systems," *Journal of Modern Power Systems and Clean Energy,* vol. 2, pp. 59-68, 2014.

[10] S. V. Dhople and A. D. Dominguez-Garcia, "Estimation of Photovoltaic System Reliability and Performance Metrics," *IEEE Transactions on Power Systems,* vol. 27, pp. 554-563, 2012.

[11] M. Theristis and I. A. Papazoglou, "Markovian Reliability Analysis of Standalone Photovoltaic Systems Incorporating Repairs," *IEEE Journal of Photovoltaics,* vol. 4, pp. 414-422, 2014.

[12] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel Model for Analyzing Coordinated Cyber-Physical Attacks on Power Systems," *IEEE Transactions on Smart Grid,* vol. 7, pp. 2260-2272, 2016.

[13] Y. Abdallah, Z. Zheng, N. B. Shroff, H. El Gamal, and T. El-Fouly, "The Impact of Stealthy Attacks on Smart Grid Performance: Tradeoffs and Implications," *IEEE Transactions on Control of Network Systems,* pp. 1-1, 2016.

[14] Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, *et al.*, "Detection of Cyber Attacks Against Voltage Control in Distribution Power Grids With PVs," *IEEE Transactions on Smart Grid,* vol. PP, pp. 1-1, 2015.

[15] Y. Xiang, Z. Ding, Y. Zhang, and L. Wang, "Power System Reliability Evaluation Considering Load Redistribution Attacks," *IEEE Transactions on Smart Grid,* pp. 1-1, 2016.

[16] Y. Zhang, L. Wang, and Y. Xiang, "Power System Reliability Analysis With Intrusion Tolerance in SCADA Systems," *IEEE Transactions on Smart Grid,* pp. 1-1, 2015.

[17] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Inclusion of SCADA Cyber Vulnerability in Power System Reliability Assessment Considering Optimal Resources Allocation," *IEEE Transactions on Power Systems,* vol. 31, pp. 4379-4394, 2016.

[18] R. Billinton and W. Li, *Reliability Assessment of Electric Power Systems Using Monte Carlo Methods*, 1994.
[19] M. Bessani, C. D. Maciel, R. Z. Fanucchi, and A. C. C. Delbem, "Impact of operators' performance in the reliability of cyber-physical power distribution systems," *IET Generation, Transmission & Distribution*, vol. 10, pp. 2640-2646, 2016.
[20] E. Zio, "Practical Applications of Monte Carlo Simulation for System Reliability Analysis," in *The Monte Carlo Simulation Method for System Reliability and Risk Analysis*, ed London: Springer London, 2013, pp. 83-107.
[21] E. P.-C. Matthew SMITH, "Cyber Risk Analysis for a Smart Grid: How Smart is Smart Enough? A Multi-Armed Bandit Approach," in *2nd Singapore Cyber Security R&D*, Singapore, 2017.
[22] R. K. Abercrombie and F. T. Sheldon, "Security Analysis of Smart Grid Cyber Physical Infrastructures Using Game Theoretic Simulation," presented at the IEEE Symposium Series on Computational Intelligence, 2015.
[23] N. J. Daras, "Stochastic Analysis of Cyber-Attacks," in *Applications of Mathematics and Informatics in Science and Engineering*, N. J. Daras, Ed., ed Cham: Springer International Publishing, 2014, pp. 105-129.
[24] R. E. Brown, *Electric Power Distribution Reliability*, Second ed.: Taylor & Francis Group, LLC, 2009.
[25] D. GmbH, "DIgSILENT PowerFactory 15, tutorial.," ed. Germany, 2013.
[26] H. Lei and C. Singh, "Developing a benchmark test system for electric power grid cyber-physical reliability studies," in *2016 International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*, 2016, pp. 1-5.
[27] H. Lei and C. Singh, "Power system reliability evaluation considering cyber-malfunctions in substations," *Electric Power Systems Research*, vol. 129, pp. 160-169, 2015.
[28] H. Lei, C. Singh, and A. Sprintson, "Reliability Modeling and Analysis of IEC 61850 Based Substation Protection Systems," *IEEE Transactions on Smart Grid*, vol. 5, pp. 2194-2202, 2014.
[29] C. Grigg, P. Wong, P. Albrecht, R. Allan, M. Bhavaraju, R. Billinton, *et al.*, "The IEEE Reliability Test System-1996. A report prepared by the Reliability Test System Task Force of the Application of Probability Methods Subcommittee," *IEEE Transactions on Power Systems*, vol. 14, pp. 1010-1020, 1999.
[30] "IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems (Gold Book)," *IEEE Std 493-1997 [IEEE Gold Book]*, pp. 1-464, 1998.
[31] W. Li, *Risk Assessment of Power Systems: Models, Methods, and Applications*, second ed., 2014.
[32] R. Billinton and S. Jonnavithula, "A test system for teaching overall power system reliability assessment," *IEEE Transactions on Power Systems*, vol. 11, pp. 1670-1676, 1996.
[33] J. N. S. Dr Rebecca Klahr, Paul Sheriffs, Tom Rossington, Gemma Pestell, Professor Mark Button and Dr Victoria Wang, "Cyber security breaches survey 2017," Ipsos MORI Social Research Institute and Institute for Criminal Justice Studies, University of Portsmouth, Department for Digital, Culture, Media & Sport of UK Government2017.
[34] D. S. Kirschen and D. Jayaweera, "Comparison of risk-based and deterministic security assessments," *IET Generation, Transmission & Distribution*, vol. 1, p. 527, 2007.