IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON IEEE POWER & ENERGY SOCIETY SECTION

Received December 18, 2019, accepted January 25, 2020, date of publication January 30, 2020, date of current version February 10, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2970598

Impact of the Integration of Information and Communication Technology on Power System Reliability: A Review

BILKISU JIMADA-OJUOLAPE[1,2] AND JIASHEN TEH[1], (Member, IEEE)
[1]School of Electrical and Electronic Engineering, Engineering Campus, Universiti Sains Malaysia (USM), Nibong Tebal 14300, Malaysia
[2]Department of Electrical and Computer Engineering, Kwara State University, Malete 241104, Nigeria

Corresponding author: Jiashen Teh (jiashenteh@usm.my)

This work was supported in part by the Ministry of Education Malaysia Fundamental Research Grant Scheme (FRGS) under Grant 203/PELECT/6071442, and in part by the USM Research University (RU) under Grant 1001/PELECT/8014099.

ABSTRACT There has been a progressive development in the synthesis of Information and Communication Technologies (ICTs) in power networks recently. ICT systems have become a vital part of every aspect of our daily lives and its integration into the electric power system has become paramount. ICTs support efficient incorporation of activities of all stakeholders of the power system to certify a more cost-effective and sustainable power system. The power system will exhibit intelligent monitoring and control, bidirectional communication between stakeholders and power system elements, security and safety of supply and self-healing qualities. However, asides from the vast benefits ICTs, their implementation within the power network come with some drawbacks which include element failures, failures due to interdependencies as well as vulnerabilities to cyber-attacks. These drawbacks can impact the reliability of the power network negatively. The objective of this paper is to investigate the impact of ICTs integration on the reliability of power networks in terms of empirical validation of standard reliability indices. This study groups the findings into four perspectives, including the effects of cyber power interdependencies, ICT infrastructure failures, cyber-attacks and environmental conditions. As expected, results show that failures and maloperations in the ICT network have adverse effects on system reliability and careful considerations need to be made to dampen these shortcomings.

INDEX TERMS Cyber power networks, cyber-physical systems, ICT, power system reliability, smart grid.

NOMENCLATURE

ADN	Active Distribution Network
CEM	Consequent Event Matrix
CI	Customer Interruptions
CML	Customer Minutes Lost
CPI	Cyber Power Interdependency
CPIM	Cyber-Physical Interface Matrix
CPS	Cyber Power Systems/ Cyber-Physical System
CPU	Central Processing Unit
CT	Current transformer
DEEI	Direct Element-Element Interdependency
DER	Distributed Energy Resources
DG	Distributed Generation
DMS	Distribution Management System
DNEI	Direct Network-Element Interdependency
DoS	Denial of Service
DR	Demand Response
DSM	Demand Side Management
EDNS	Expected Demand Not Served
EENP	Expected Energy Not Produced
EENS	Expected Energy not Supplied
EFLC	Expected Frequency Load Curtailment
EMU	Energy management unit
FACTS	Flexible AC transmission systems
FMEA	Failure Mode Effect Analysis
FOR	Forced Outage Rate
HREC	Hormozgan regional electrical company
ICT	Information and Communication Technology
IED	Intelligent Electronic Device
LOLE	Loss of Load Expectation
LOLP	Loss of Load Probability
LR	Load Redistribution
MIS	Markov chain Imbeddable Structure

The associate editor coordinating the review of this manuscript and approving it for publication was Ning Kang.

NAN	Neighbourhood-Area Network
OHL	Overhead Line
PMU	Phasor Measurement Unit
PSMC	Pseudo-Sequential Monte Carlo
PT	Potential Transformer
RBTS	Roy Billinton Test System
RES	Renewable Energy System
RTS	Reliability Test System
SAIDI	Average number of DG interruptions
SAIFI	Average duration of DG interruptions
SCADA	Supervisory control and data acquisition
SG	Smart Grid
SIPS	System Integrity Protection Scheme
SMCS	Sequential Monte Carlo Simulation
SSI	System Security Index
SSSC	Static Synchronous Series Compensator
SU	System Unavailability
TVLR	Time-Varying Line Rating
WAMS	Wide Area Measurement System
λ	Failure rate
μ	Repair rate

I. INTRODUCTION

There is currently an upward incline in interests on the deployment of Smart Grid. Even more, so is the rapid development of the integration of ICT systems in power networks. ICT systems have become a vital part of every aspect of our daily lives and its integration into the electric power system has grown paramount to match the increasing demand on the power system.

The electric grid is a centralized internetwork of all parts including but not limited to generators, transformers, substations and transmission lines that deal with the generation of electrical energy, the transmission of power over very long distances and distribution of electrical power from various load hubs [1]. The current grid structure, which is lacking in reforms for as many as 100 years, is very complex and delivers energy with one-way power flow [2]. The grid is gradually getting to its limits in meeting up with the steadily increasing demand for electricity. Hence, it has become essential to boost reliability. This situation has called for a paradigm shift from the conventional grid to a more reliable Smart Grid (SG) or a modern cyber power internetwork that will utilize the application of digital processing and ICTs to efficiently incorporate the activities of all stakeholders of the power system. Shifting towards a smarter grid ultimately certifies a more cost-effective and sustainable power system that will exhibit intelligent applications like intelligent monitoring and control, bidirectional communication between stakeholders and power system elements, security and safety of supply and self-healing qualities [1]–[4]. Fig 1 is a structural example of a smart grid showing the power and ICT networks, bidirectional communication features as well as intelligent applications.

Implementation of ICTs enable power system operators to be better efficient. Some of the direction for

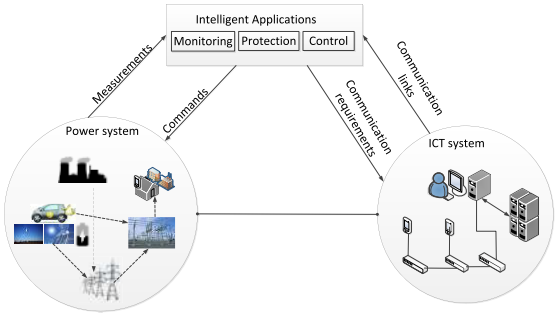

FIGURE 1. Modern cyber power internetwork.

ICT implementation include Interoperability of bidirectional communication technologies between different infrastructure devices within the power system Demand-side management programs, Open Architectures for EVs, MGs and other DERs, Standards and protocols are guiding the interoperability of ICT in power systems and Cybersecurity measures [4]. All these ICT perspectives can be deployed to cater to such system requirements as situational awareness, planning and operations and flexibility to accommodate increased numbers of DERs on the distribution system as well as to improve processes and self-healing during downtimes [4].

Reliability in power systems is an important characteristic which accurately measures the probability of a system to adequately function for a required period and under specific or variable operating conditions [5]. The primary function of a power system is to supply electricity to connected consumers, and significant stakeholders in the power sector all strive to achieve this primary purpose.

In modern power systems, there is a fundamental need for all stakeholders including energy generators, transmission network owners and operators, energy distributors to be aware of the required standard to which they must operate to attain optimum reliability of the overall power system. So, there are different requirements in the form of reliability measures which are unique to each stakeholder of the power system [6]. Reliability studies generally discuss two basic functional system states. The first state, termed adequacy, is the presence of required facilities to supply the energy that the customers expect and have demanded without the consideration of system disturbances. The second system state also is known as security refers to the capability of the power system to deal with sudden disturbances like loss of system components, line faults or whatever form of abnormality that may exist within the system [7].

Implementation of ICTs in the power network significantly boosts power system reliability. Chances are that situational awareness will be more accurate when the network presents intelligent applications like intelligent monitoring, protection and control, two-way real-time communication, which brings the prospect of making adequate decisions to operate the power system efficiently. Adequate awareness ultimately improves the reliability of the power system to a significant extent. However, ICT implementation involves integrating

the power network with new elements and features which are also prone to failure at some point. So, reliability studies need to consider the individual reliability of these ICT elements in order not to jeopardize the overall power system reliability. Moreover, ICT implementation involves the network to be in active connection to the internet, which also poses other threats like cyber-attacks. This paper reviews studies which address the impact of ICT on the reliability of power systems.

This paper aims to present findings from current literature about the impact of ICT implementation on the power system reliability. In the remainder of the article, section II briefly describes ICT in power systems, section III presents the findings of the literature review, section IV itemizes some current issues, and the paper concludes in section V.

II. ICT IN POWER SYSTEMS

The current electricity network structure is highly complex and has remained unchanged for decades and as such, become a hindrance to the advancement of the electricity supply chain. Currently, most of the grid's power flows are unidirectional sourced from a centralized pool of power generation facilities where the reliability is ensured by having a reserve capacity. This mainstream approach increases the generation capacity to meet the increasing electricity demand. The lack of infrastructural change, growing population, climate change, poor visibility, slow response times, lack of situational awareness has made the grid inefficient and less reliable and as such deterred the evolution of the power sector [3]. China alone consumed about 1138TWh of electricity in 2000, and this figure rose to 4921TWh in 2015 [8]. Forecasts show an increase in electricity consumption by 4.2% annually until 2022 [1]. The grid thus needs to be transformed into a more intelligent internetwork to accommodate the ever-growing demand.

Smart Grid is an internetwork of electrical power components that can efficiently incorporate the activities of all its stakeholders including but not limited to generators, transmission lines and the electricity consumers to certify a more cost-effective, flexible, reliable and sustainable power system. A requirement to transform the current grid to a smart state is the implementation of ICT to ensure a bidirectional cyber-physical system where all stakeholders of the network are in active communication thereby promoting intelligent monitoring and control and self-healing qualities by the grid [4], [9]. The smart grid aims to decrease the pressure on the current power grid by decentralizing the generation sources and influencing usage patterns of electricity consumers to make them more conscious in energy conservation by launching programs such as Demand Side Management (DSM). It improves the reliability of the power network by improving fault detection and self-healing without the involvement of any personnel. It also improves the flexibility of the system to be able to incorporate distributed energy resources (DERs) such as renewable energy sources like wind, hydro and solar generation, as well as controllable loads. It also aims to electrify the transport sector, for example, electric vehicles, incorporate energy storage systems onto the grid to compensate during peak demand periods, encourage the development of smart cities, as well as boost the general efficiency and sustainability of the power grid [1], [3], [10].

The presence of ICT infrastructure within the power system provides an avenue by which the power systems can more efficiently manage its overall increased complexity and size. Due to the accessibility to reliable bidirectional real-time data on the state of the power system, the possibility to operate within narrower limits of security has become possible. ICT presence decreases the frequency and duration of supply interruptions and has contributed to a reduction of total operation costs [11].

Failures can occur in the ICT system within the power network at any point. These malfunctions of the ICT components can lead to the determent of the adequacy functionality of the power grid. Possibly due to a subsystem getting an incorrect or inadequate data needed for performing the normal operation or a delay/failure in sending a load or dispatch control signal. A dependence on ICT systems can significantly increase the weakness and exposure of the power network to threats and malicious attacks. So, the ability of the power network to maintain confidentiality, availability and integrity despite the prevailing disturbances is a crucial focus for modern power systems [12]. The reliability indices are quantified to assess the situation while considering both the combined ICT and power system infrastructure holistically [13]. There are four major categories of ICT within the power system, namely; Acquisition, communication, processing and Implementation subsystems [11], [14], [15]. Fig. 2 shows the categories and their relationship.

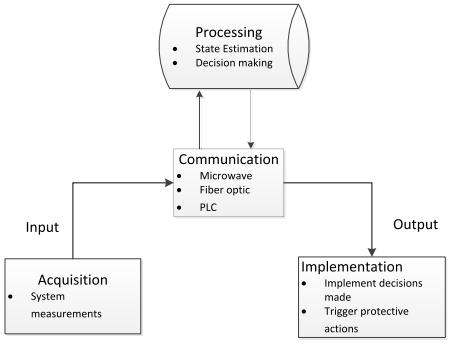

FIGURE 2. Categories of ICT in the power network.

a. Acquisition: collects instantaneous system status data like power flow measurements, CB status, bus voltage and frequency measurements, the status of switching devices and delivers these data to the processing subsystem via the communication subsystem.
b. Processing: assesses the data received from the acquisition subsystem to determine the state of the power network and informs the operator of the real-time system state. A state estimator is an essential tool in the processing subsystem

that gives reliable representations of the power network based on the input from the acquisition subsystem. The results from the state estimator are used to make adequate decisions for implementation.

c. Implementation: uses the results from the system processing to carry out necessary actions like triggering protective relays and circuit breakers after detection of a fault on the power network.

d. Communication: this is the medium through which all other subsystems coordinate within the power network either via wired or wireless channels.

A. CYBER-POWER INTERDEPENDENCIES

The modern power systems which consist of a hybrid cyber network and physical power network are typically called cyber-power networks. As such, interdependencies exist between elements and networks within the hybrid system implying that the functionality of a component or a network impacts the functionality of components in/or the other network in the larger hybrid system [16]. Four types of interdependencies generally classified into two subgroups, namely; direct interdependency and indirect interdependency. The classification of the interdependencies depends on the location of failures within the cyber network. Fig 3 represents a cyber-power hybrid network showing both networks tightly coupled together, various elements of each network as well as the different categories of interdependencies that exist.

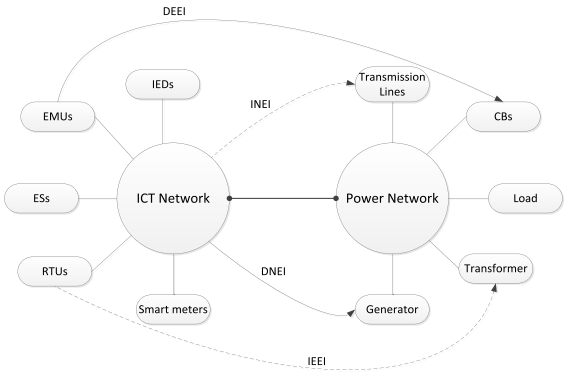

FIGURE 3. Cyber-power network.

1) DIRECT INTERDEPENDENCY

This group of interdependency ensures real-time operation in the power network and is classified into two subgroups.

a. Direct Element-Element Interdependency (DEEI): maloperations of elements in one network results in the maloperation of components in the other network [17]. DEEI occurs at points of physical connections between the cyber and power network elements. In fig 3, DEEI between EMUs and CBs are shown indicating that a maloperation of the EMU in the cyber network causes a failure of the CB in the power network, which can cause widespread outages. DEEI represents the most basic form of interdependency.

b. Direct Network-Element Interdependency (DNEI): the performance of one network impacts an element in the other system [17]. As shown in fig 3, a failure in a communication link in the cyber network can cause a mis operation of a generator in the power network.

Applications of direct interdependencies include loss of stability and control as well as the loss of operation within the hybrid network. Article [18] describes these applications in detail.

2) INDIRECT INTERDEPENDENCY

These are more complex relationships than direct interdependencies. Maloperations of a cyber network or its element indirectly impact the functionality of a power network or its element [16]. When a failure occurs in the cyber system or its element, the power network still functions, but the impact of the failure presents potential future failures in the power network or the loss of certain functionalities/capacities.

a. Indirect Element-Element Interdependency (IEEI): Failures occur in cyber elements that are in physical connection with a power element. However, this does not deter the power element from functioning optimally at the instant of failure; rather, the power element is at risk of possible future failure [19]. In fig 3, if an RTU malfunctions, this could mean that a particular monitoring function has failed. The failure could result in an impaired situational awareness which does not affect the functionality of the power element at the instant but can present an increased likelihood of maloperation in the power element subsequently.

b. Indirect Network-Element Interdependency: Failures occur within the cyber network but does not directly and immediately affect a power element. It rather makes the power element prone to subsequent failures [19]. For instance, if there is a failure in the communication link that gives information to the protection system, it means a protective device will lack information at the instant of a subsequent fault which could damage the element in the power system.

This paper reviews various articles which have studied the impacts of various interdependencies mentioned above on power system reliability and synthesizes the results in section III.

III. LITERATURE REVIEW

The literature review is conducted to answer the following questions to achieve the aim of checking the impacts of ICTs on power system reliability;

a. What is the actual numerical measure of the effect that penetration of ICTs has on standard reliability indices to determine the overall impact on system reliability?

b. What case studies and probabilistic modelling techniques are in current usage for assessment of the relationship between ICT and power systems?

In the review process, three databases IEEE, Science Direct and Scopus, were examined from the year 2000 till date. The search yielded a significant number of full-length journal and conference proceeding articles. The study considers the following inclusion criteria while selecting the papers for final review;

a. The study addresses relationships between ICTs and power systems.
b. The study demonstrates probabilistic modelling techniques in analysis.
c. The article evaluates the reliability of the power system by giving actual measures of standard reliability indices.

A. SYNTHESIS OF FINDINGS

This subsection presents findings on the impact of ICT on reliability from existing literature. The reviewed studies classify into four perspectives based on individual themes. These groups are; cyber power interdependencies, cyber-attacks, infrastructure failures and weather and environmental conditions. This paper also examines the case studies/cyber network components, reliability evaluation methods for the ICT subsystem as well as the overall impact of ICT on the power network in each article.

B. IMPACT OF CYBER POWER INTERDEPENDENCIES

As previously explained in section II, two primary groups of interdependencies exist in cyber power networks. These interdependencies whether direct or indirect has an impact on the overall reliability of the larger network. Article [17] demonstrates failures from direct interdependencies, and it determines that reliability dwindles more from faults in the ICT network than in the power network. It also shows that ring topologies with redundant features could increase reliability indices compared to other structural arrangements of cyber network components. In [20] three topologies bus, ring and star were also tested in a system with DG of wind and diesel to improve the overall reliability. It concludes that communication devices, such as switches could effectively influence system adequacy.

Monitoring and protection systems are applications of indirect CPIs. Article [19] demonstrates the effect of indirect CPI and results show that not taking the monitoring and protection system into account during reliability studies poses a threat to the overall reliability of the power system. Failures in both subsystems could also potentially decrease overall system reliability. Table 1(A) enumerates findings of notable studies on the impact of direct CPIs on system reliability, table 1(B) shows findings of studies on the impact of indirect CPIs while table 1(c) shows the findings of the impact of both direct and indirect CPIs. On table 1(c), authors in [18] compare the impact of direct and indirect CPIs and found that information exchange between both CPIs makes them interconnected which shows the importance of studying both types of CPIs simultaneously.

C. IMPACT OF CYBER ATTACKS

The inclusion of ICTs in power networks comes with certain drawbacks, one of which is the vulnerability to cyber-attacks such as the violation of communication protocols to tamper with information availability. Such attacks are called Denial of Service attacks (DoS) and they can be deployed at various levels of the communication within the power network. False data injection, intrusion, phishing, sabotage and terrorism are also common types of attacks against the power system. The recent false data injection cyber-attack on Ukrainian distribution grids in 2015, motivated the governments to perceive cyber-attacks as a national security issue and moved to make power networks stealthier [25]. Attacks capitalize on the vulnerability of the security system of the networks and are mostly caused by injecting false data to tarnish the system integrity.

Cyber-attacks can impact the power network either directly or indirectly. For direct impact, an incorrect command is sent to a cyber element to cause the primary infrastructure to function incorrectly thereby resulting in a system blackout while in indirect effect, wrong measurement information is sent to the cyber component to tamper with the decision making of the system [26]. SCADA/EMS and CBs are typical targets of cyber-attacks because the SCADA is responsible for monitoring the situational awareness of the system, and the CB directly controls the operations of essential network elements. Cyber-attacks negatively impact the cost, efficiency and overall reliability of power networks. In article [27], the impact of various types of cyber-attack on power system operations such as state estimation voltage control and automatic generation control are reviewed.

Articles [28], [29] study the impact of load redistribution attacks. LR attack is when an attacker injects wrong data to a localized part of the system to tamper with the state estimation of the network to avoid detection and to cause chaos. Once there is misinformation about the real-time state of the network, operators make wrong decisions based on incorrect state estimation results which may be detrimental to the operations of the power network. Article [30] addresses malicious tripping of wind turbines in wind farms in which attackers intrude on the system by sending spurious commands to the SCADA/EMS to cause widespread disruption in electricity supply. Tables 2(A) and(B) specify the results of these and other notable studies considering cyber-attacks.

D. IMPACT OF ICT INFRASTRUCTURE FAILURES

Where ICT elements are increasingly becoming a great part of the modern power system, possibilities of their failures must be put into consideration so appropriate planning can be done to avoid adverse effects on power system reliability. Author [37] classifies the reliability of ICT equipment into functional and network failures because the two states have varying results when considering intelligent applications. Functional failures cause the ICT element to be unable to execute a command which can further lead to loss of situational

TABLE 1. (a) Impact of direct cyber power interdependency on power system reliability. (b) Impact of indirect cyber power interdependency on power system reliability.

(A)

Source	Contribution	Limit	Case study/ cyber network components	Reliability Evaluation	Impact on reliability
[17]	New algorithm proposed to assess the impact of direct CPIs of communication and power networks on network reliability. Method proposed improves reliability.	Model does not include consideration for indirect. The method used requires much computation and not feasible for the assessment of a larger network.	Microgrid test system comprised of 4 DG units and 3 loads in radial topology. ES, EMU, server	P-Table, cyber-power link and state mapping.	Reliability dwindles by a factor of more than eight times from failures in the ICT system than that in the power system alone. Ring topologies with redundant EMUs can decrease EENS by 8%, 0.4%, 77% compared to basic ring, redundant star and bus counterparts respectively.
[20]	Presents an analytical method based on the effect of cyber failures on the power network while optimizing cyber network structure to improve reliability.	Considers only direct CPIs. Assessed a specific localized network.	Real modernized 20kV distribution system of HREC of Iran. EMU, switch and CPU.	State mapping, state probability.	Switches can effectively influence system adequacy. Mesh topology of the cyber network decreases EENS by about 27%, 15%, 19% in bus, ring and star topologies respectively.
[21]	Proposed a novel analytical method to evaluate the direct cyber failure impacts on power network reliability based on different types of DG penetration. Method used improves reliability.	Does not consider indirect CPI. Assessed a specific localized network.	20Kv distribution network of HREC Iran. EMUs, servers, switches.	State mapping, State probabilities, Weibull model for wind behaviour, segmentation concept.	Increasing the DG penetration level decreases EENS thereby improving the overall reliability of the power network.

(B)

Source	Contribution	Limit	Case study/ cyber network components	Reliability Evaluation	Impact on reliability
[19]	Proposes a reliability evaluation algorithm to model indirect CPIs and check its impact on network reliability. Method proposed improves reliability.	Model only applicable to indirect CPIs. The method used requires much computation and not feasible for the assessment of a larger network.	High voltage substation with monitoring and protection systems. Protection unit, monitoring unit, switch.	P-Table, State updating.	Unavailability of monitoring and protection system increases EENS by 82%. While failures in both monitoring and protection systems increase EENS by as much as 3.24%.
[23]	Developed a new model for the CB based on indirect interdependencies between the intelligent measurement and the CB. State generating method also proposed to consider optimal operation strategy in island MGs. Reliability is increased by using this method.	The proposed method takes a longer computational time (about 99 secs more) to calculate the reliability indices.	RBTS Bus 6 F4. Controllers, IEDs, CT, Intelligent Measurement, optical fibre, switch.	SMCS	EENS decreases by a maximum value of 38.4%, which verifies the effects of communication network on microgrids reliability.
[24]	Developed a new model to check the validity of a cyber link with dynamic routing, delay and communication error and to assess the effect of automation functionality faults in the cyber network on distribution network reliability. Method used offers improvement of reliability.	The paper focuses only on indirect interdependencies.	Typical distribution network consisting of PV and storage units. ES, server, IEDs, optical fibre cables.	Non SMCS.	Distribution network reliability is strongly affected by cyber network traffic.

TABLE 1. *(Continued.)* **(c) Impact of both direct and indirect cyber power interdependency on power system reliability.**

(C)

Source	Contribution	Limit	Case study/ cyber network components	Reliability Evaluation	Impact on reliability
[18]	Discusses and compares both direct and indirect CPIs impact on power system reliability using mathematical reliability models. Focused more on verifying the impact rather than improving reliability.	Assessed a specific localized network. The method used requires much computation and not feasible for assessment of a larger network.	High voltage substation. IEDs	State updating.	A nearly linear increase in LOLE as the λ increases in both direct and indirect CPIs; therefore, reliability is impacted negatively by the failure of the IEDs.
[22]	Proposes an analytical reliability model that considers the impact of both physical and cyber improvements on overall reliability and checks the effect of adding more interdependency. Method focused on investigating effects on reliability and not its improvement.	MIS method used has high computational complexity.	IEEE 14-bus test system. PMUs, SSSCs, Communication channel.	Markov chain imbeddable structure.	Quantitative analysis shows that introducing additional interdependency degrades the system reliability by a significant factor.

awareness capability for monitoring and control by the EMS. While in network failures, the ICT element remains functional but fails at processing external commands. ICT elements can fail to send correct control, demand response, load shed, open/close command, measurement, and status data signals to their respective terminals [38]. Failures could also occur while processing a fault as well as Cyber-induced dependent failures (CDFs). Tables 3(a)-(c) show the results of studies that assess the effect of failures in the cyber network infrastructure on network reliability.

E. IMPACT OF WEATHER AND ENVIRONMENTAL CONDITIONS ON ICTS

Rainstorms and other adverse weather conditions can impact the communication signal in a power system negatively. The movement of cloud patterns can also influence renewable energy generation significantly. Topographical and meteorological conditions can also increase the noise level in ICT transmission mediums. All these factors can impact the reliability of the power network severely.

Articles [53] and [54] employ a meteorological model to simulate local weather conditions that can attenuate the performance of ICT wireless Wi-Max networks to determine the reliability of ADNs. In article [12], data from weather station monitoring systems in a UK based ADS trial project were sampled for 28 days to determine the reliability of the monitoring system by examining the effect of weather changes on real-time thermal rating. Table 4 shows the results of these studies.

F. CASE STUDIES

Several case studies have been used to demonstrate the process of reliability evaluation of power networks. In the reviewed studies, several standardized test networks are used in the evaluation process. The IEEE and RBTS test systems are very popular in the reviewed studies constituting over 60% of the examined papers. The standard test systems are developed for the purpose of research to aid the process of reliability evaluation in generation and composite systems and to be able to compare techniques used for reliability analysis. The basic system data required for reliability assessment are provided in these test networks [56], [57]. Authors use these test networks by adding ICT extensions to the existing standardized system thereby allowing them to carry out reliability evaluation. Researchers also commonly use very simple developed networks for assessment such as in [11], [17] and seven other studies. Another group of studies used real networks for the assessment of reliability. In [20] and [21] the 20kV distribution system of HREC of Iran was used as their case study while in [42] a real hydropower station in the UK was featured.

G. RELIABILITY EVALUATION METHODS IN CYBER-POWER NETWORKS

The reliability assessment of power systems can either be carried out using Analytical or simulation methods [5], [7]. Reliability assessment is deployed to assess the economic effect of power system failures. Modelling techniques first used in practical applications were all deterministic. Analytical methods use mathematical models to determine the reliability metrics. These methods can be bulky and impractical when large scale networks with very complex schemes are involved [58]. Simulation techniques on the other hand, usually based on Monte Carlo methods, consider the actual process and random behavior of system components included and have been used in many studies to

TABLE 2. (a) Impact of cyber-attacks on power system reliability. (b) Impact of cyber-attacks on power system reliability.

(A)

Source	Contribution	Limit	Case study/ cyber network components	Reliability Evaluation	Impact on reliability	Reliability Improvement
[26]	Proposed a model to check the network reliability considering cyber-attacks to the IEDs and the distribution main station.	Paper focuses on only attacks on IEDs and distribution main station.	IEEE 33-bus distribution system. IEDs, distribution main station.	SMCS	The attack on IEDs has a more significant impact on network reliability than that on the distribution main station. SAIDI and EENS rise by about 71% and 77% respectively.	No. focused on checking impact of cyber-attack scenarios.
[28]	Proposes an adequacy evaluation procedure incorporating load redistribution attack considering physical failures and a model representing the attack.	Paper considers only the immediate load redistribution attack.	IEEE 14-bus system. Smart meters	Bilevel and trilevel optimization problem, SMCS	A rise in the attack level and the number of attacks can worsen the power system reliability inversely, an increase in the defence level improves the reliability. A system with adequate transmission capacity can maintain its reliability while under LR attacks.	Yes. Increase in defence levels boosts reliability.
[29]	Presents a mathematical bilevel optimization problem where the power law distribution represents local LR attacks, evaluates centralized attack regions and deduces its impact on reliability.	Attack regions between 5 and 8 lines only were considered in this study.	IEEE 14-bus system. Generators, transmission lines.	Bilevel optimization problem, SMCS	The frequent occurrence of local LR attack dramatically impacts the reliability of the system. The behaviour of the attacker also has an essential influence on reliability. LR attack can lead to an increase in EENS by as much as almost 13%.	No. focused on examining impact of failures from LR attack.
[31]	Proposed a technique that integrates reliability of physical components and the effect of cyber-attacks against breakers considering the behaviour of the devices and attackers.	The study divides attacks into mainstream, organized and terrorist threats and considers only the first two groups.	IEEE RTS79 system. CBs.	Attack probability, SMCS	Protecting crucial components from cyber-attacks is vital. An increase in attacks implies a decreased system reliability, while a more considerable increase with more resources is even more harmful.	No. focused on checking impact of failures of CBs from cyber-attack.
[30]	Presents a quantitative analysis for assessing power system reliability incorporating cyber-attacks on wind farm SCADA/EMS systems, causing wind turbines to trip off.	Assumes that the cyber attackers can get the absolute minimum state security in this study.	IEEE RTS79 SCADA/EMS	Bayesian attack graphs, SMCS	At attack level 1, LOLP and EENS increase by almost 5% and 8% respectively. These values verify that power system reliability degrades with an increase in cyber-attacks and even more so an upgrade in the attack level.	No. focused on examining impact of cyber-attack on wind farms SCADA/EMS systems.

(B)

Source	Contribution	Limit	Case study/ cyber network components	Reliability Evaluation	Impact on reliability	Reliability Improvement
[32]	Proposes a mathematical framework to assess power system reliability in a cyber-physical system with multiple photovoltaic (PV) system configurations.	The study assumes that attacks are categorized into three intensity levels and impact the status of the system.	IEEE RTS79 RBTS MU, ES, line protection panel.	Non SMCS	There are considerable impacts on PV operation from cyber threats. In all case studies presented, an increase in PV generation decreases the EENS by a significant amount.	Yes. Increased PV penetration improves reliability.
[33]	Proposes an optimal strategy to evaluate power system reliability while considering unidentifiable cyber-attack.	Focuses only on the unidentifiable attack scenario.	IEEE 14-bus SCADA	SMCS	There is a linear relationship between reliability and the attack magnitude, resource and frequency. As these parameters increase, LOLP and EENS increases by about 0.0025 and 250MWh/y respectively.	No. checks the impact of unidentifiable attack on system reliability.

TABLE 2. *(Continued.)* **(b) Impact of cyber-attacks on power system reliability.**

[34]	Examines the cyber architecture of unified power flow controller considering possible cyber-attack scenarios to determine its impact on system reliability.	Focuses mainly on the EENS and doesn't quantify load shedding.	RBTS Unified power flow controller.	Attack tree, SMCS	EENS degrades when the controller is attacked and even more to a greater degree when the frequency of attack is doubled. However, EENS is improved by 0.86% when recovery time is halved.	Yes. Proposes that a reduction in recovery time improves system reliability.
[35]	Analyses the DoS, confidentiality and integrity of SCADA system considering 10 types of attack scenarios such as DoS, worms and man in the middle attacks to determine impact on power system reliability.	Quantifies only FOR, LOLP and does not measure EENS.	IEEE RTS 79 and modified RTS SCADA	SMCS	In all scenarios analysed, reliability dwindles as both occurrence and severity of attack increases. Worms have the greatest impact on reliability while DoS attacks has the least impact.	No. Examines the impact of attack scenarios on reliability.
[36]	Study evaluates the SCADA system based on 6 types of attack scenarios to check impact on system reliability.	Quantifies only FOR, LOLP and does not measure EENS.	IEEE RTS 79 SCADA	Bayesian attack graph, SMCS	An increase in the success frequency and attack level causes a large decline in the values of LOLP in all scenarios studied. There is also a negative impact on the FORs of the generators and transmission lines hence reliability is impacted negatively.	No. Examines the impact of attack scenarios on reliability.

analyze large amounts of system states for large iterations of simulations [59], [60]. Although computational times are significantly longer in simulation methods, these techniques permit a high degree of complexity in system modelling while considering the practical essence of the derived reliability indices [7].

Fig 4 depicts a high-level process in the simulation method for reliability assessment. The process begins by inputting data samples in form of failure rates, repair rates and other network data. Next the process checks for failures by sampling and then uses probabilistic techniques to carry out analyses. Finally, after convergence reliability indices which represent the output of the process are computed. These indices represent the empirical value of economic impact of network reliability and importantly, presents adequate information for system planning.

The conventional reliability assessment techniques, which primarily focus on the power network separately from the ICT infrastructure are well researched into and quite mature. However, reliability assessment of the cyber part of the system in conjunction with the power network is still in its early stages with much work yet undone. The setback is that these methods primarily focus on the power network while assuming that the ICT network is 100% reliable. Because of the rise in the level of ICT integration, it is proving to be impractical and counterproductive to make such assumptions [12].

Different researchers have proposed diverse methods to model the ICT network, such as state mapping and updating, modified Markov chains. However, these methods do not adequately quantify the actual state of all ICT parts of the CPS.

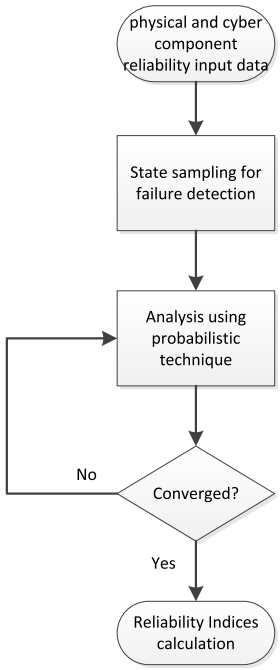

FIGURE 4. High level process flow in Simulation technique for reliability studies.

Other studies have developed more comprehensive methods with the researchers saddled with the extra task of modifying test networks with ICT extensions for specific single use. Moreover, these test networks only account for small localized networks which lack the generality and applicability to depict the actual reliability of the broader composite system.

TABLE 3. (a) Impact of ICT infrastructure failures on power system reliability. (b) Impact of ICT infrastructure failures on power system reliability.

(A)

Source	Contribution	Limit	Case study/ cyber network components	Reliability Evaluation	Impact on reliability	Reliability Improvement
[11]	Proposes a methodology to assess power system reliability (security) by considering Interruption as a delay in operator reaction because of ICT failure.	Study asses a small system, and reliability data used was not realistic.	2 bus transmission system.	SMCS	Increase in λ of the ICT system leads to an increase in load shedding, increase in μ leads to reduced load disconnection and improved reliability.	Yes. Method used shows that an increase in μ improves reliability.
[39]	Developed a methodology that permits the real-time implementation of the effect of ICT failures on TVLR OHLs network reliability.	Simulation is restricted to only OHLs and TVLR-ICT failures while generators and FACTS are assumed fully reliable. Impractically, all ICT components are assumed to have equal failure/repair rates.	IEEE-RTS 96 network. TVLR-ICT	SMCS	Correct deployment of ICT helps to improve EFLC by a double fold while EENS is also enhanced by approximately 20%.	Yes. Reliability enhancement is offered by this method.
[40]	Developed a new approach that emphasizes on connections of the ICT system, intelligent applications and time dependencies of power demand for calculation of network reliability.	In the ICT system, no analogue analysis was possible due to the lack of statistical data. System-wide reliability indices not measured.	MV distribution grid with a mainly open-loop ring topology. Processors, optical fibre cables and SCADA.	FMEA, Markov process	Use of intelligent applications may be of benefit to some customers. However, extensive reinforcement of the power system can also have adverse effects on reliability.	Yes. Approach enables system operators plan more efficiently.
[41]	Proposes a Non SMCS method for systems involving dependent failures which requires less computational and storage resources than the SMCS method.	Due to the large size of the composite system, it is impractical to use Non SMCS method to deduce the joint probability distribution of all components before sampling.	RBTS with extensions of cyber part at buses 3 to 5. Communication signals.	Non SMCS, CPIM, CEM.	Proposed method improves efficiency compared to pure SMCS. EENS and CPU time is reduced by less than 5% and 60% respectively.	Yes.
[42]	Introduces a new vulnerability index (SSI) to quantify the impact of failure or maloperation of ICT network components on power network reliability in a real power network intertrip scheme.	Measures only the vulnerability of the ICT components. Assumed communication channels are fully reliable.	Real hydropower station in the UK. Main Protection Trip Relay, RTU, Programmable Logic Control, CB.	Complex network theory.	The complex network model is more scalable and more accessible to implement than conventional analysis methods. Results affirm that failures in ICT infrastructure worsen system reliability.	No. focused on proposing a more efficient tool for reliability assessment.

(B)

Source	Contribution	Limit	Case study/ cyber network components	Reliability Evaluation	Impact on reliability	Reliability Improvement
[43]	Evaluates the reliability of the cyber-physical system involving the effects of failures in the monitoring function on the power system.	Does not evaluate the impact of component differences on the system reliability.	IEEE 30-bus system. Monitoring system.	Non SMCS, Reliability block diagram.	The reliability index increases significantly, thereby decreasing the reliability of the system due to the impact of the monitoring function failure. EENS worsens by a factor of 76% as a result of the failure.	No. focused more on the examination of reliability impact due to failure.
[44]	Proposed static connection and dynamic transmission models to assess the effects of the cyber system on power distribution operation reliability while introducing System Unavailability index.	The proposed method may not be applicable due to the high cost of deployment.	RBTS Bus 6 IED, optical fibre, switches, server, optical network terminal.	Fault tree model, SMCS.	Cyber components with high failure rates have a significant impact on distribution network reliability regardless of being a key node. Failures in the cyber element severely increase EENS by 212.05%.	No. method quantifies reliability impact of cyber component failure.

TABLE 3. *(Continued.)* **(b) Impact of ICT infrastructure failures on power system reliability. (c) Impact of ICT infrastructure failures on power system reliability.**

[45]	Presents a functional representation of ICT to consider the effect of ICT infrastructure failure on distribution network reliability.	The proposed method does not extensively represent the presence of ICT within the distribution network.	Overhead medium-voltage distribution feeder. Control centre, telecoms switches and RTUs.	SMCS	Existing non-homogenous dependence between various ICT elements and the distribution network.	No. Emphasizes the effect of ICT infrastructure failure on reliability.
[46]	Assessment method proposed to check the impact of frequency control malfunction of Cyber components on network reliability.	Paper considers only first-order faults in cyber elements.	RBTS Bus 6 F4 System. Controllers, Public Coupling Connector, PT, CT, switches, optical fibre cables.	SMCS	Random failures of cyber elements cause a drastic increase in EENS by 269.31% in comparison with random misoperations of power elements. Smaller frequency fluctuation ranges also lower system reliability.	No. focused on checking the impact of element failures on MG reliability.
[47]	Implemented a methodology to evaluate the reliability of an extended 4-bus substation layout with ethernet based protection scheme considering cyber link failures.	Only first-order primary faults considered.	4-bus substation. CB, PT, CT, IED, Ethernet cable.	CEM, CPIM	Undesired trips because of cyber link failures have a significant negative impact on network reliability.	No. focused on reliability assessment considering link failures.

(C)

Source	Contribution	Limit	Case study/ cyber network components	Reliability Evaluation	Impact on reliability	Reliability Improvement
[48]	Developed a co-simulation platform focused on modelling ICT devices to analyze the impact of reliability issues on energy production in ADNs.	Models ICT network as a black box which does not necessarily allow the highest degree of simulation detail.	Rural network based on ATLANTIDE project. DMS, WiMax antenna, router, IED.	Co-simulation	Failures of ICT control and communication leads to a rise in energy curtailment. EENS is about 122% higher in a passive network without ICT features.	No. Focused on developing a co-simulation tool for reliability assessment.
[49]	Proposes a reliability assessment technique using the event tree model to assess the impact of cyber system failure on fault processing in cyber-physical distribution systems.	The study considers only transmission delays as against considering other network performance evaluation indices.	RBTS Bus 6 system. Switches, IEDs.	SMCS Event tree model.	Improper fault location causes an increase in the power outage area, which adversely impacts the supply capacity at load points resulting in increased outage times. Incorrect fault location in the fault tree accounts for more than 50% of the EENS value.	No. focused on examining the impact of improper fault location on reliability.
[50]	Developed a model to account for cyber-enabled feeders in the upstream substation to determine the effect of cyber-physical integration on reliability in distribution systems. Analysed substation layouts to reduce the impact of CDF on reliability.	Partitions Twenty-two zones for the simplification of the minimal path.	Modified RBTS Bus 2 RTU, CT, PT, ES, protection IEDs, feeder terminal units, communication links.	Non SMCS	Results show that reliability is impacted positively by the integration of ICT in distribution systems as against the shortcomings of CDF. CDF impact falls as the automation level increases.	Yes. study examines the impact of CPI vulnerabilities on reliability.
[51]	Proposes a communication network reliability model for a DTR system that features redundancies and line operation policies to improve the availability of the communication network to a significant extent.	Study does not consider infrastructure failures due to cyber-attacks or natural disasters.	IEEE 24-bus network. NAN connection.	SMCS	There is a continuous increase in the value of EENS with a decreasing NAN gateway availability. Additional redundancies (three and four) only improves EENS by less than 1% showing that creating such redundancies has very little to no effect on the improvement of reliability.	Yes. Proposed addition of redundancies to improve reliability.

TABLE 3. *(Continued.)* **(c) Impact of ICT infrastructure failures on power system reliability.**

[52]	Proposes a method to show the effect of limitation of either or both situational awareness and controllability on composite system reliability.	WAMS is assumed to be the sole system in charge of monitory and control for the power system. The protection system is considered fully reliable.	9-bus system and IEEE 57-bus PMU, CT, PT, Communication link.	SMCS	In the 57-bus network, EDNS is increased by 41% and 28%, when WAMS failures are incorporated as well as when control functions are provided through other means respectively. While in the 9-bus network EDNS is 5.12% higher when considering contingencies in WAMS network.	No. Addresses the impact of failures in WAMS network.

TABLE 4. **Impact of environmental conditions on power system reliability.**

Source	Contribution	Limit	Case study/ cyber network components	Reliability Evaluation	Impact on reliability	Reliability Improvement
[12]	The research uses monitored weather data to evaluate the real-time thermal rating of overhead lines in a distribution network.	Checks only reliability based on the station downtime for a short period of 28 days.	UK based ADS trial project. SCADA	Co-simulation	Most of the GPRS based weather stations experienced significantly longer downtimes than hard-wired stations with just 5 mins downtown and reliability of 99.99% due to signal strength and lower bandwidth with the lowest presenting reliability of 85.71%.	Yes. Reduces the impact of communication reliability on overall system reliability.
[53], [54]	Employed a new meteorological model to simulate the impact of rain fade on the performance of ICT wireless networks to determine the reliability of ADNs.	Considers only the impact of the wireless communication outage on the reliability of the ADN. Empirical approach used due to the absence of comprehensive information on occurrence probabilities of different weather conditions.	A typical scenario of real distribution networks in rural areas. WiMax	PSMC	96% reliability of the ICT system improves the EENP, SAIDI and SAIFI by about 77%, 90% and 67% respectively.	No. study focused on developing efficient reliability assessment tool.
[55]	Discussed a DR scheme to increase the 11kV distribution network capacity utilization implemented in both radial and ring configurations.	The study provides only CI and CML system performance indices used in the UK. Other Reliability indices not specified.	Two test distribution networks using specific numerical applications to real UK networks. WiMax	SMCS	Implementation of DR potentially increases network utilization without the need to change present configuration provided NOP remains closed, thereby improving reliability.	Yes. Proposed configuration offers an improvement of reliability.

The literature review shows that 58% of the studies examined favored the conventional sequential Monte Carlo simulation methods while incorporating some analytical methods like the event tree, fault tree, CPIM and CEM to name a few. Five articles used the non SMCS method while two articles [53], [54] used the PSMCS method. Articles [12], [48] present a co-simulation tool which refers to the simulation of both cyber and power network concurrently to assess reliability. This permits detailed ICT modelling with power networks in a holistic assessment. Furthermore, seven studies present purely analytical methods such as state mapping and updating, and complex network theory mainly to assess relatively small power networks. Table 5 lists some notable techniques used in the examined studies for cyber system reliability assessment.

H. POWER SYSTEM RELIABILITY INDICES

In reliability studies, probability of a system to function adequately under specified conditions are measured.

As explained in section I, all stakeholders within the three hierarchies of the electric power system have a required standard to which they must operate to attain optimum overall reliability. This is in the form of reliability measures which are unique to each stakeholder of the power system. Reliability analysis typically consist of three broad stages: state selection, state evaluation and finally index calculation [61]. These measures are generally called reliability or adequacy indices. Reliability evaluation is carried out by using a wide range of methods such as those mentioned in subsection G above, after which reliability indices are calculated. These indices represent the measure of reliability of power systems.

TABLE 5. Notable Methods for Cyber system reliability assessment from reviewed literature.

Source	Method	Definition	Merits	demerits
[11], [23], [24], [28]–[31], [39], [44]–[46], [51], [52], [55]	SMCS	Simulates actual system performance and random behaviour in chronological order.	Permits a high level of modelling complexity	Highly time consuming.
[24], [32], [41], [43], [50]	Non SMCS	Randomly selects system states for sampling during simulation.	Requires less memory and computational time.	Not as comprehensive as the SMCS method because it cannot directly provide frequency and duration reliability metrics.
[53], [54]	PSMCS	This is a joint method of simulation where Non SMCS is used for failure states selection and SMSC used to analyse the non-failure states that represent the total system interruption.	Enhances the efficiency and accuracy of the reliability assessment process and saves some computational time.	Requires more computational effort.
[17]–[21]	State mapping State updating	Represents a process in which the probability of a failure in cyber element translates to an element failure or malfunction in the power network.	Presents the possibility of running two heterogeneous networks.	Complex computational technique and not practicable for reliability assessment of large networks.
[22]	Markov Chain Imbeddable structure (MIS)	Analytical method for the assessment of reliability of a system with known component reliability values.	Applicable methods available to reduce complexity is possible through state elimination and other methods.	High computational complexity.
[44], [49]	Fault Tree, Event Tree	Top to bottom, left to right structure that uses logic to combine previous level factors to perform failure analysis of an undesired system state.	Direct logic relationships which make identification of cause and effects of failures simpler.	Requirement of complex computational time and effort which increases exponentially with the size of the network.
[42]	Complex Network Theory	Permits the modelling of hybrid cyber and power networks as a graph composed of several nodes and edges.	More scalable and more accessible implementation than conventional analysis methods.	Difficult to deploy on large networks.
[33]	Reliability Block diagram	This is a diagrammatic representation of components logical relationship.	Simple implementation.	Not practicable on real networks.
[41], [47]	CPIM CEM	CEM shows effect of communication failure scenarios on power components and CPIM shows their corresponding probabilities.	Considers the effect of cyber component failures on the power system to a great extent.	Requires great computational effort and time.

Majority of these indices represent expected values of a random variable which is not actually a deterministic measure. They are average values of the examined occurrence over a long period of time [62]. These expected values are considered sufficient in indicating adequacy status of a system because they show factors such as system component availability and capacity, load characteristics and uncertainty, system configurations and operational conditions [62]. The deduced indices assist utilities and system operators to plan adequately and make the right decisions to enhance the operations of power systems [63].

In generating system reliability assessment, some of the commonly used indices are Loss of Load Probability (LOLP), Loss of Load Expectation (LOLE), Loss of Energy Probability (LOEP), Loss of Energy Expectation (LOEE), and Loss of Load Frequency (LOLF) and Loss of Load Duration (LOLD).

In composite reliability assessment, some indices such as Expected Energy Not Served (EENS), Expected Frequency of Load Curtailment (EFLC), Expected Demand not Supplied (EDNS), Expected Energy not Produced (EENP) and Probability Load Curtailment (PLC).

In distribution system evaluation, indices such as SAIFI, SAIDI, CAIFI, ASAI as well as ENS are commonly used as measures of reliability [7], [62].

Generally, the most commonly used indices are the LOLE, LOLP, EENS, SAIFI and SAIDI as evidenced in this paper from the reviewed studies. These indices [7], [62] are explained below.

a. LOLE is the average number of days or hours in given period of usually a year in which the available generating capacity becomes less than the daily peak or hourly load.
b. LOLP is the probability that the available generation will be insufficient to meet the load demand. LOLP just defines the likelihood of days of trouble but does not give the measure of severity.
c. EENS represents the ratio of the unserved expected energy in the duration of a long period of examination to the total energy demand during that same period.

EENS has the longest convergence time compared to other indices ensuring that the right number of samplings have been carried out [64], [65].

d. SAIFI is a customer-based index that gives information about the average frequency of interruptions that a customer would experience.
e. SAIDI is also a customer based index which is the average outage time that a customer experiences.

IV. CURRENT ISSUES

This section presents some current issues in the study of ICT impact on power system reliability.

a. Impact of different adverse weather conditions on ICT infrastructure in the generation and composite power systems to determine its effects on overall power system reliability still needs further research. Although some studies are available in this area, it still requires more attention from researchers.
b. New research needs to consider additional factors in evaluating the impact of local LR attacks on system adequacy. More investigation should also be done on methods to defend the power system against LR attacks.
c. Standard test systems that include ICT infrastructure are currently unavailable. This makes the comparison of methods to assess their efficiency challenging. Generic testbeds need to be developed to encourage a more unified and standard performance evaluation of CPS. Studies [66] and [67] made efforts of developing a benchmark test system for CPS.
d. Studies assessing the impact of System Integrity Protection Scheme on power system reliability is yet to be fully mature. Research [68] proposes a risk assessment method to check the effect of undesirable interactions between SIPS and the results show that malfunctions in SIPS pose an increased risk to system integrity. Article [69] presents a technique based on Markov modelling for risk assessment of SIPS maloperations in power system. In studies [15], [70], [71], Markov modelling and Fault Tree Analysis were used for component-level reliability analysis of generic SIPS. The studies cited above don't mainly evaluate the effect of implementing SIPS on the reliability of the broader composite network.

V. CONCLUDING REMARKS

The tight coupling of the ICT and power network in the cyber power network will significantly increase the efficiency and overall reliability of the system while also presenting potential risks of failures at some point which has adverse negative impacts on the overall reliability of the power network. Implementation of ICT allows effective management of the increased complexity of modern power systems with enhanced capabilities of operating within narrower limits due to the improvement of situational awareness capabilities. Operators can make better and quicker decisions regarding network functions which ultimately saves costs and decreases frequency and duration at which supply interruptions occur. System planners must give adequate attention to these ICT factors in the planning stages of the power network. ICT could be a potential disadvantage to the power network. However, if it is considered adequately in the planning stages with the infusion of necessary redundancies, its benefits to the broader network reliability far outweigh its shortcomings. The presence of ICT reduces the levels of standard reliability metrics such as EENS as evidenced in the examined studies.

REFERENCES

[1] K. G. Di Santo, E. Kanashiro, S. G. Di Santo, and M. A. Saidel, "A review on smart grids and experiences in Brazil," *Renew. Sustain. Energy Rev.*, vol. 52, pp. 1072–1082, Dec. 2015.
[2] S. Supriya, M. Magheshwari, S. Sree Udhyalakshmi, R. Subhashini, and Musthafa, "Smart grid technologies: Communication technologies and standards," *Int. J. Appl. Eng. Res.*, vol. 10, no. 20, pp. 16932–16941, 2015.
[3] B. Panajotovic, M. Jankovic, and B. Odadzic, "ICT and smart grid," in *Proc. 10th Int. Conf. Telecommun. Mod. Satell. Cable Broadcast. Serv. (TELSIKS)*, Oct. 2011, pp. 118–121.
[4] M. Sooriyabandara and J. Ekanayake, "Smart grid—Technologies for its realisation," in *Proc. IEEE Int. Conf. Sustain. Energy Technol. (ICSET)*, Dec. 2010, pp. 1–4.
[5] R. Billinton, R. N. Allan, R. Billinton, and R. N. Allan, *Reliability Evaluation of Engineering Systems: Concepts and Techniques*. New York, NY, USA: Plenum Press and Pitman, 2013.
[6] R. Allan and R. Billinton, "Probabilistic assessment of power systems," *Proc. IEEE*, vol. 88, no. 2, pp. 140–162, Feb. 2000.
[7] R. Billinton and R. N. Allan, *Reliability Evaluation of Power Systems*. New York, NY, USA: Plenum Press and Pitman, 1986.
[8] D. A. Tillman and D. A. Tillman, "Introduction: The overarching issues," in *Coal-Fired Electricity and Emissions Control: Efficiency and Effectiveness*. Oxford, U.K.: Butterworth-Heinemann, 2018, pp. 1–27.
[9] I. A. Tøndel, J. Foros, S. S. Kilskar, P. Hokstad, and M. G. Jaatun, "Interdependencies and reliability in the combined ICT and power system: An overview of current research," *Appl. Comput. Inform.*, vol. 14, no. 1, pp. 17–27, Jan. 2018.
[10] M. Masera, E. F. Bompard, F. Profumo, and N. Hadjsaid, "Smart (electricity) grids for smart cities: Assessing roles and societal impacts," *Proc. IEEE*, vol. 106, no. 4, pp. 613–625, Apr. 2018.
[11] M. Panteli and D. S. Kirschen, "Assessing the effect of failures in the information and communication infrastructure on power system reliability," in *Proc. IEEE/PES Power Syst. Conf. Expo. (PSCE)*, Mar. 2011, pp. 1–7.
[12] J. Taylor, S. Jupe, G. Celli, and F. Pilo, "Assessing the impact of ICT on the reliability of active distribution systems," in *Proc. 22nd Int. Conf. Electr. Distrib.*, 2013, p. 1370.
[13] R. Siqueira de Carvalho and S. Mohagheghi, "Analyzing impact of communication network topologies on reconfiguration of networked microgrids, impact of communication system on smart grid reliability, security and operation," in *Proc. North Amer. Power Symp. (NAPS)*, 2016, pp. 1–6.
[14] T. Bjorn, M. Fontela, P. Mellstrand, R. Gustavsson, C. Andrieu, and S. Bacha, "Overview of ICT components and its applications in electric power systems," in *Proc. 2nd Int. Conf. Crit. Infrastructures*, 2004, pp. 10–15.
[15] Y.-C. Hsiao, J. López, T.-Y. Hsiao, and C.-N. Lu, "Considering ICT in reliability assessment of system protection scheme," in *Proc. 18th Int. Conf. Intell. Syst. Appl. Power Syst. (ISAP)*, 2015, pp. 1–6.
[16] B. Falahati and Y. Fu, "A study on interdependencies of cyber-power networks in smart grid applications," in *Proc. IEEE PES Innov. Smart Grid Technol. (ISGT)*, Jan. 2012, pp. 1–8, 2012.
[17] B. Falahati, Y. Fu, and W. Lei, "Reliability assessment of smart grids considering direct cyber-power interdependencies," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1515–1524, 2012.
[18] B. Falahati, S. Kahrobaee, O. Ziaee, and P. Gharghabi, "Evaluating the differences between direct and indirect interdependencies and their impact on reliability in cyber-power networks," in *Proc. IEEE Conf. Technol. Sustain. (SusTech)*, Jan. 2018, pp. 1–6.
[19] B. Falahati and Y. Fu, "Reliability assessment of smart grids considering indirect cyber-power interdependencies," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1677–1685, Jul. 2014.

[20] A. H. Ahangar and H. A. Abyaneh, "Improvement of smart grid reliability considering various cyber network topologies and direct interdependency," in *Proc. Asia–Pacific Power Energy Eng. Conf. (APPEEC)*, Dec. 2016, pp. 267–272.
[21] A. H. Ahangar, H. A. Abyaneh, and G. B. Gharepetian, "Negative effects of cyber network (control, monitoring, and protection) on reliability of smart grids based on DG penetration," in *Proc. 5th Int. Conf. Comput. Knowl. Eng. (ICCKE)*, 2015, pp. 54–60.
[22] K. Marashi, S. S. Sarvestani, and A. R. Hurson, "Consideration of cyber-physical interdependencies in reliability modeling of smart grids," *IEEE Trans. Sustain. Comput.*, vol. 3, no. 2, pp. 73–83, Apr. 2018.
[23] J. Guo, W. Liu, F. R. Syed, and J. Zhang, "Reliability assessment of a cyber physical microgrid system in island mode," *CSEE J. Power Energy Syst.*, vol. 5, no. 1, pp. 46–55, 2019.
[24] W. Liu, Q. Gong, H. Han, Z. Wang, and L. Wang, "Reliability modeling and evaluation of active cyber physical distribution system," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 7096–7108, Nov. 2018.
[25] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.
[26] B. Chen, Z. Lu, and H. Zhou, "Reliability assessment of distribution network considering cyber attacks," in *Proc. 2nd IEEE Conf. Energy Internet Energy Syst. Integr.*, Oct. 2018, pp. 1–6.
[27] K. Chatterjee, V. Padmini, and S. A. Khaparde, "Review of cyber attacks on power system operations," in *Proc. IEEE Int. Symp. Technol. Smart Cities (TENSYMP)*, Jul. 2017, pp. 1–6.
[28] Y. Xiang, Z. Ding, and L. Wang, "Power system adequacy assessment with load redistribution attacks," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2015, pp. 1–5.
[29] Z. Ding, Y. Xiang, and L. Wang, "Quantifying the influence of local load redistribution attack on power supply adequacy," in *Proc. IEEE Power Energy Soc. Gen. Meet.*, Jul. 2016, pp. 1–5.
[30] Y. Zhang, Y. Xiang, and L. Wang, "Power system reliability assessment incorporating cyber attacks against wind farm energy management systems," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2343–2357, Sep. 2017.
[31] Y. Xiang, L. Wang, and Y. Zhang, "Power system adequacy assessment with probabilistic cyber attacks against breakers," in *Proc. IEEE Power Energy Soc. Gen. Meet.*, Jul. 2014.
[32] H. Gunduz and D. Jayaweera, "Reliability assessment of a power system with cyber-physical interactive operation of photovoltaic systems," *Int. J. Electr. Power Energy Syst.*, vol. 101, pp. 371–384, Oct. 2018.
[33] Z. Ding, Y. Xiang, and L. Wang, "Incorporating unidentifiable cyber-attacks into power system reliability assessment," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Aug. 2018, pp. 1–5.
[34] Y. Xiang, Y. Zhang, L. Wang, and W. Sun, "Impact of UPFC on power system reliability considering its cyber vulnerability," in *Proc. IEEE Power Eng. Soc. Transmiss. Distrib. Conf.*, vol. 1, Apr. 2014, pp. 1–5.
[35] Y. Zhang, L. Wang, and W. Sun, "Investigating the impact of cyber attacks on power system reliability," in *Proc. IEEE Int. Conf. Cyber Technol. Autom. Control Intell. Syst. (IEEE-CYBER)*, May 2013, pp. 462–467.
[36] Y. Zhang, Y. Xiang, and L. Wang, "Reliability analysis of power grids with cyber vulnerability in SCADA system," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2014, pp. 1–5.
[37] D. D. Schacht, H. Vennegeerts, S. Krahl, and A. Moser, "Evaluation of reliability in distribution grids depending on information and communication technology," in *Proc. Influence Intell. Appl. ICT-Syst.*, 2015, pp. 56–63.
[38] R. S. De Carvalho and S. Mohagheghi, "Impact of communication system on smart grid reliability, security and operation," in *Proc. 48th North Am. Power Symp. (NAPS)*, 2016, pp. 1–6.
[39] C. Cruzat and K. Kopsidas, "Modelling of network reliability of OHL networks using information and communication technologies," in *Proc. IEEE Manchester PowerTech, Powertech*, Jun. 2017, pp. 1–6.
[40] D. Schacht, D. Lehmann, H. Vennegeerts, S. Krahl, and A. Moser, "Modelling of interactions between power system and communication systems for the evaluation of reliability," in *Proc. 19th Power Syst. Comput. Conf. (PSCC)*, Jun. 2016, pp. 1–7.
[41] H. Lei and C. Singh, "Non-sequential Monte Carlo simulation for cyber-induced dependent failures in composite power system reliability evaluation," *IEEE Trans. Power Syst.*, vol. 32, no. 2, pp. 1064–1072, May 2017.
[42] W. Zhu, M. Panteli, and J. V. Milanovic, "Reliability and vulnerability assessment of interconnected ICT and power networks using complex network theory," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Aug. 2018, pp. 1–5.
[43] M. Ni and M. Li, "Reliability assessment of cyber physical power system considering communication failure in monitoring function," in *Proc. Int. Conf. Power Syst. Technol. (POWERCON)*, 2019, pp. 3010–3015.
[44] S. Wang, Z. Wu, A. Su, S. Jin, Y. Xia, and D. Zhao, "Reliability modeling and simulation of cyber-physical power distribution system considering the impacts of cyber components and transmission quality," in *Proc. Chin. Control Conf. (CCC)*, Jul. 2018, pp. 6166–6171.
[45] T. Chaudonneret, H. Decroix, and J. D. F. McDonald, "Representation of the influence of telecommunications on electrical distribution network reliability," in *Proc. IEEE 3rd Int. Conf. Smart Grid Commun. (SmartGridComm)*, Nov. 2012, pp. 258–263.
[46] J. Guo, T. Zhao, W. Liu, and J. Zhang, "Reliability modeling and assessment of isolated microgrid considering influences of frequency control," *IEEE Access*, vol. 7, pp. 50362–50371, 2019.
[47] H. Lei, C. Singh, and A. Sprintson, "Reliability analysis of modern substations considering cyber link failures," in *Proc. IEEE Innov. Smart Grid Technol.-Asia (ISGT ASIA)*, Nov. 2015, pp. 1–5.
[48] M. Garau, G. Celli, E. Ghiani, G. G. Soma, F. Pilo, and S. Corti, "ICT reliability modelling in co-simulation of smart distribution networks," in *Proc. 1st IEEE Int. Forum Res. Technol. Soc. Ind. (RTSI)*, Sep. 2015, pp. 365–370.
[49] Y. Liu, L. Deng, N. Gao, and X. Sun, "A reliability assessment method of cyber physical distribution system," *Energy Procedia*, vol. 158, pp. 2915–2921, Feb. 2019.
[50] H. Yuan, G. Li, Z. Bie, and M. Arif, "Distribution system reliability assessment considering cyber-physical integration," *Energy Procedia*, vol. 158, pp. 2655–2662, Feb. 2019.
[51] J. Teh and C.-M. Lai, "Reliability impacts of the dynamic thermal rating system on smart grids considering wireless communications," *IEEE Access*, vol. 7, pp. 41625–41635, 2019.
[52] F. Aminifar, M. Fotuhi-Firuzabad, M. Shahidehpour, and A. Safdarian, "Impact of WAMS malfunction on power system reliability assessment," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1302–1309, Sep. 2012.
[53] G. Celli, E. Ghiani, F. Pilo, and G. G. Soma, "Reliability assessment in smart distribution networks," *Electr. Power Syst. Res.*, vol. 104, pp. 164–175, Nov. 2013.
[54] G. Celli, E. Ghiani, F. Pilo, and G. G. Soma, "Impact of ICT on the reliability of active distribution networks," in *Proc. IET*, 2012, p. 367.
[55] A. L. A. Syrri and P. Mancarella, "Reliability evaluation of demand response to increase distribution network utilisation," in *Proc. Int. Conf. Probabilistic Methods Appl. Power Syst. (PMAPS)*, Jul. 2014, pp. 1–6.
[56] P. F. Chairman, M. P. Bhavaraju, and B. E. Biggerstaff, "IEEE reliability test system: A report prepared by the reliability test system task force of the application of probability methods subcommittee," *IEEE Trans. Power App. Syst.*, vol. PAS-98, no. 6, pp. 2047–2054, Nov. 1979.
[57] P. F. Chairman, M. P. Bhavaraju, and B. E. Biggerstaff, "IEEE reliability test system-1996. A report prepared by the reliability test system task force of the application of probability methods subcommittee," *IEEE Trans. Power Syst.*, vol. 14, no. 3, pp. 1010–1020, Aug. 1999.
[58] A. Escalera, B. Hayes, and M. Prodanović, "A survey of reliability assessment techniques for modern distribution networks," *Renew. Sustain. Energy Rev.*, vol. 91, pp. 344–357, Aug. 2018.
[59] J. Teh, "Adequacy assessment of wind integrated generating systems incorporating demand response and battery energy storage system," *Energies*, vol. 11, no. 10, p. 2649, Oct. 2018.
[60] J. Teh, C.-M. Lai, N. A. Muhamad, C. A. Ooi, Y.-H. Cheng, M. A. A. M. Zainuri, and M. K. Ishak, "Prospects of using the dynamic thermal rating system for reliable electrical networks: A review," *IEEE Access*, vol. 6, pp. 26765–26778, 2018.
[61] H. Abunima, J. Teh, C.-M. Lai, and H. Jabir, "A systematic review of reliability studies on composite power systems: A coherent taxonomy motivations, open challenges, recommendations, and new research directions," *Energies*, vol. 11, no. 9, p. 2417, Sep. 2018.
[62] R. Billinton and L. Wenyuan, *Reliability Assessment of Electric Power Systems Using Monte Carlo Methods*. New York, NY, USA: Springer, 1994.
[63] F. Mohamad and J. Teh, "Impacts of energy storage system on power system reliability: A systematic review," *Energies*, vol. 11, no. 7, p. 1749, Jul. 2018.
[64] J. Teh, C.-M. Lai, and Y.-H. Cheng, "Impact of the real-time thermal loading on the bulk electric system reliability," *IEEE Trans. Rel.*, vol. 66, no. 4, pp. 1110–1119, Dec. 2017.
[65] J. Teh, "Uncertainty analysis of transmission line end-of-life failure model for bulk electric system reliability studies," *IEEE Trans. Rel.*, vol. 67, no. 3, pp. 1261–1268, Sep. 2018.

[66] H. Lei and C. Singh, "Developing a benchmark test system for electric power grid cyber-physical reliability studies," in *Proc. Int. Conf. Probabilistic Methods Appl. Power Syst. (PMAPS)*, 2016, pp. 1–5.
[67] H. Lei, Y. Chakhchoukh, and C. Singh, "Framework of a benchmark testbed for power system cyber-physical reliability studies," *Int. Trans. Elect. Energy Syst.*, vol. 29, no. 1, p. e2692, Jan. 2019.
[68] N. Liu and P. Crossley, "Assessing the risk of implementing system integrity protection schemes in a power system with significant wind integration," *IEEE Trans. Power Del.*, vol. 33, no. 2, pp. 810–820, Apr. 2018.
[69] M. Panteli and P. Crossley, "Impact of SIPS performance on power systems integrity," in *Proc. Int. Conf. Adv. Power Syst. Autom. Protection (APAP)*, vol. 1, 2011, pp. 280–285.
[70] M. Panteli, P. A. Crossley, and J. Fitch, "Quantifying the reliability level of system integrity protection schemes," *IET Gener., Transmiss. Distrib.*, vol. 8, no. 4, pp. 753–764, Apr. 2014.
[71] M. Panteli and P. A. Crossley, "Reliability assessment of SIPS based on a safety integrity level and spurious trip level," in *Proc. IET Conf.*, 2012, pp. 1–7.

BILKISU JIMADA-OJUOLAPE received the B.Sc. degree (Hons.) in electrical engineering and electronic engineering from the Kwame Nkrumah University of Science and Technology, Kumasi, Ghana, in 2011, and the M.Sc. degree in systems engineering from Loughborough University, Loughborough, U.K., in 2013. She is currently pursuing the Ph.D. degree with the School of Electrical and Electronic engineering, Universiti Sains Malaysia.

She worked with the Nigerian Electricity Regulatory Commission (NERC) for about a year, where she was involved in license application evaluation for Independent Power Producers and Inspection of substations within Abuja, Nigeria, amongst other duties. She was also a National System Engineer with the NTA-Star TV Network (StarTimes), where she was managing the operations of ten cities and was also part of a think tank committee that was brainstorming new products for the company. She joined Kwara State University (KWASU) afterwards, in 2015. Her current research interests are in renewable energy, power systems, smart grid reliability, ICTs in smart grid, and small hydropower generation.

Mrs. Jimada-Ojuolape is a member of the Association of Practicing Women Engineers in Nigeria (APWEN) and the Nigerian Society of Engineers (NSE) and certified by the Council for the Regulation of Engineering in Nigeria (COREN).

JIASHEN TEH (Member, IEEE) received the B.Eng. degree (Hons.) in electrical and electronic engineering from Universiti Tenaga Nasional (UNITEN), Selangor, Malaysia, in 2010, and the Ph.D. degree in similar field from the University of Manchester, Manchester, U.K., in 2016.

Since 2016, he has been a Senior Lecturer/ Assistant Professor with the Universiti Sains Malaysia (USM), Penang, Malaysia. In 2018, he was appointed and served as an Adjunct Professor with the Green Energy Electronic Center, National Taipei University of Technology, Taipei Tech., Taipei, Taiwan. Since 2019, he has also been an Adjunct Professor with the Intelligent Electric Vehicle and Green Energy Center, National Chung Hsing University (NCHU), Taichung, Taiwan. His research interests include probabilistic modeling of power systems, grid-integration of renewable energy sources, and reliability modeling of smart grid networks.

Dr. Teh is a Chartered Engineer (CEng) conferred by the Engineering Council, U.K., and The Institution of Engineering and Technology (IET), a member of the IEEE Power and Energy Society, The Institution of Engineers Malaysia (IEM), and a Registered Engineer in the Board of Engineers Malaysia (BEM). He received the outstanding publication awards from USM, in 2017 and 2018. He is also a regular invited Reviewers of the *International Journal of Electrical Power and Energy Systems*, IEEE Access, the IEEE Transactions on Industry Applications, the IEEE Transactions on Vehicular Technology, the IEEE Transactions on Reliability, the IEEE Transactions on Industrial Electronics, and the *IET Generation, Transmission and Distribution*.