Supervisory Energy-Management Systems for Microgrids: Modeling and Formal Verification

Sugumar, Gayathri; Selvamuthukumaran, Rajasekar; Novak, Mateja; Dragicevic, Tomislav

Published in:
I E E E Industrial Electronics Magazine

DOI (link to publication from Publisher):
10.1109/MIE.2019.2893768

Publication date:
2019

Document Version
Accepted author manuscript, peer reviewed version

Modeling and Formal Verification of Supervisory Energy Management Systems for Microgrids

Abstract: This paper presents the modeling and verification of supervisory energy management systems (EMS) for microgrids using timed automata (TA) and formal verification approach. EMS plays an essential role in managing the power flow among different components in the microgrid system for its safe and reliable operation. The modeling of EMS is based on pre-defined invariants with allowable and non-allowable operating modes, which are the conditions that do not change over time. The failure of invariants could have severe effects on the microgrid system functionality, which highlights the importance of verification during the initial stage of EMS design. Conventional approaches such as simulation and/or experimental verification requires manual checking and skilled professional knowledge to check EMS design correctness. Also, there may exist a corner case leading to system failure going unidentified by manual analysis. This paper proposes an automatic formal verification approach which is exhaustive and provides much stronger confidence to EMS design correctness than the conventional verification. The verification in this paper is performed using the UPPAAL model checker, a powerful toolbox for verifying real-time systems modeled as a network of timed automata. Nevertheless, the proposed approach is generic and any other commercial or non-commercial model checking tool could be used as well. The dynamics of the microgrid system components are modeled as TA where the models interact with each other through shared variables and synchronizing channels. The microgrid system considered for this study has a photovoltaic (PV) array, a pair of battery energy storage systems (BESes), a diesel generator and a load. To evaluate the proposed methodology, the timed automata model of microgrid components with supervisory controller is presented and the results show that the proposed approach is effective in verifying the EMS design.

I. Introduction

Global warming and strict energy policies have increased the awareness about the consumption of fossil fuels in many countries, stimulating the rapid promotion and usage of renewable energy sources (RES) for power generation [1]. The power electronics technology plays an important role in integration of RES into grid connected and standalone applications, as well as microgrids [2]. In recent years, microgrids have received a lot of attention as they can locally aggregate energy sources and consumers and thus make a way for more efficient power flows in the overhead modern power systems. Due to the rapid development in control strategies and technology progress, advanced microgrid are becoming a reality

today [3], [4]. A detailed survey about architectures, standardization and control strategies of microgrid applications are discussed in [5], [6]. In particular, control of microgrids can be divided in several control levels. Primary control is responsible for local current and voltage control, as well as for power sharing between the paralleled sources. Secondary control can restore the global voltage to nominal value, and minimize power sharing errors. Finally, tertiary control, also referred to as the energy management system (EMS) is concerned about optimizing the system performance by improving its intelligence level. There are many existing works on energy management system, most of them are designed heuristically and tested only for a limited set of operating conditions through simulations and/or experiments. In [7], an energy management systems for microgrid designed for a stand alone droop controlled microgrid was verified through experiment. In [8], the authors used simulation to verify the control strategies for islanded microgrid operations. The authors in [9], power management of multiple distributed generation microgrid systems is modelled to evaluate interaction of components in the system. Research work on mode changes in microgrid include multi-agent architecture to distribute energy resources in multiple microgrid [10]; load sharing among distributed generators under various load conditions [11]; and controller for residential power level microgrid system [12]. A supervisory control for a hybrid system is assessed through computer simulation in [13]. Experimental validation is used to validate voltage-power droop/frequency-reactive power boost (VPD/FQB) control scheme in [14]. Coordinated control of distributed generators in islanded and grid connected DC microgrid is verified through simulation in [15]. Simulation or experiments have been dominantly used to test the energy management systems for microgrid.

Most of the available EMS is based on logic-oriented approaches i.e., microgrid's operating modes are chosen according to pre-defined rules usually designed only by intuition. While those EMS systems allow microgrid systems to operate fairly efficient and economical, their performance is not guaranteed. The microgrid system has two distinct modes of operation: grid-connected mode and islanded mode, and they are both widely discussed in the literature [16], [17]. When microgrid system operates in islanded mode, the challenging problem is to meet the load demand and balance the energy flow between RES and BESes under any condition [18]. There are situations where the islanded mode of operation is intentionally deployed for safety and economic reasons or during maintenance sessions e.g., remote off-grid electric power systems, military based power systems, or shipboard power systems [19], [20]. In the islanded mode of operation, the controller monitors and changes the modes of individual components to maintain the power balance in the microgrid. In real time conditions, the supervisory controller enables the microgrid system to operate in different modes of operation along with different functionalities such as power quality improvement, reactive power compensation and ancillary services. For instance, when maximum power needs to be extracted from the photovoltaic's (PV), it operates in maximum power point tracking

(MPPT) mode. The PV can also work in the MPPT OFF mode if there is a surplus of energy production and the battery energy storage systems (BESes) are full. To this end, BESes can either be in charging, discharging or be in idle state. The regulated BES charging and discharging operation modes are activated to improve lifetime of the battery [19]. These different operating modes can be easily embedded in the formal verification scheme to test the controller leading to a stable system in all operating conditions.

Today, the most common approach to test all the possible modes of microgrid operation is to perform simulation and/or experiments [21], [22]. Although simulation is advantageous for testing/verification, it may not be possible to check all possible behaviours of the system [23]. Another possible way is to build the system physically, and verify its behavior directly on implemented hardware. However, failure of the test case due to design or implementation errors can cause significant damage and expense to the microgrid system. In addition to aforementioned problem, it also requires a skilled professional to check the correctness of shifting the modes of operation.

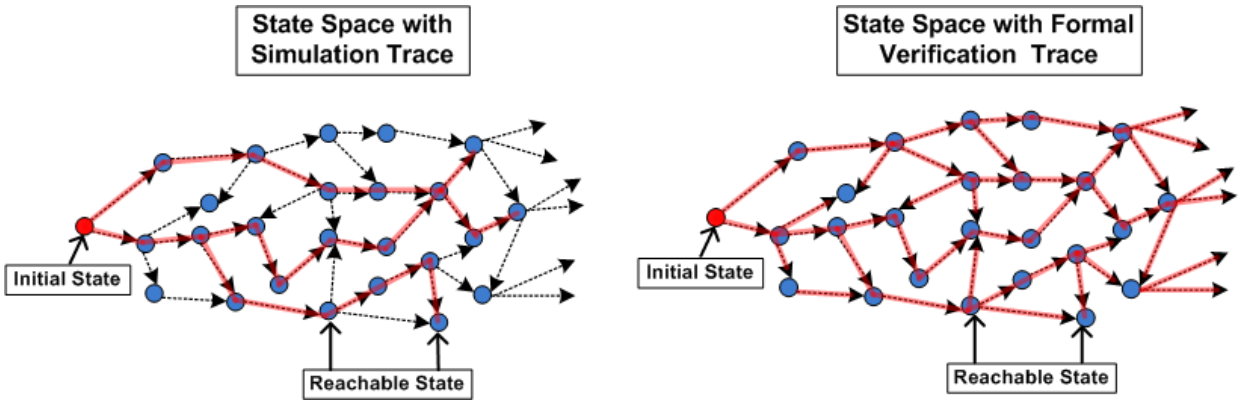

Fig. 1: State space with simulation and formal verification trace.

The paper builds upon earlier work presented in [24], by introducing formal verification to check the correctness of microgrid EMS design. Formal verification is an automatic verification approach, which explores the whole state space of the system to verify testing properties and it increases our confidence of system design correctness [25]. Fig. 1 illustrates an example of the state space path traces executed during simulation and formal verification approach. Here the edges represent the operating modes, while the vertices represent the transitions from one mode to another. In the simulation trace, the system starts from an initial state and traverses through multiple paths based on the conditions on the edges connecting the subsequent states. The conditions on the edges are influenced by the input and other environment variables. Based on the conditions, the trace of the simulation evolves by traversing to other reachable states in the system. Though many reachable states exist in the entire state space, a simulation trace may overlook some transitions or states and this indicates that the property is not verified in the entire state space. The formal verification approach explores all possible paths and exhaustively verifies all the

properties, whereas the simulation only guarantees the properties under a certain number of paths that designer could think of, but these may or may not cover the entire state-space.

Through this work, formal verification is explored to verify energy management system for microgrids. This allows for the first time systematic exploration of all possible operating conditions in a microgrid, thus being able to formally verify the correct design of its energy management system. Formal verification has been extensively used in software engineering to verify programs and applications. In recent years, formal verification has been observed to gain interest for different domains. In OS multicore power management, dynamic power management (DPM) schemes were formally verified in [26]. Authors in [27] have used formal methods to verify power-down control in audio/video components in UPPAAL. Formal methods for design and analysis of re-configurable machining systems in manufacturing industry was presented in [28]. The recent improvements in formal methods and increase in computing power have motivated researchers and engineers to verify their system through formal verification, yet it is not explored for energy management system in microgrids. In energy and power domains, formal verification have been used to analyse and verify wind turbine systems in [29]. Stability analysis of communication system in a network control system using formal methods was explored in [30]. Stochastic hybrid modelling of a microgrid is shown in [31], but formal verification of the microgrid model is not presented. To the best of authors' knowledge, this work would be the first effort to showcase energy management system modelling using timed automata and formal verification for microgrids.

Several modeling techniques are available in the literature for modeling a real time system e.g. hybrid automata, I/O automata [32], [33]. Most formal modeling methods can capture the system property, which has discrete behavior e.g. ON/OFF switching of the diesel generator. However, such methods may not be suitable to model the continuous behavior of the system such as *how long a diesel generator should remain in ON/OFF state, to maintain optimum scheduling time.* On the contrary, TA is a formal modeling technique that can capture qualitative and timing constraints of the system model needed to model and verify the microgrid system. A wide range of applications of TA are found in industrial control systems, communication protocols, and cyber physical systems [34], [35]. Since finite state automata are not expressive enough to capture the dynamics of the system, we settle to utilize TA to model microgrid. Today, there exists several tools for modeling and performing analysis of real time systems such as Romeo [36], PRISM [37], SPIN [38]. Each model checker use different combination of modelling language and properties language; while they perform the formal verification on the system model. UPPAAL [32] is a model checker, which supports TA modeling. It consists of modelling, simulator and verifier component. The system is modelled as a network of timed automata models, where each model represents a process/function or a component. The non-deterministic models interact through real-valued clocks

(timing), communication channels and shared variables. The transitions in the model are governed by guards for edges and invariants for states. During a transition from one state to other, it may issue a synchronising signal to guarantee invocation of a transition in another instance of automata in the system. The sending channel is suffixed with "!" while the receiving channel is suffixed with "?" i.e., for a channel 'ch',the sender labels channel as 'ch!' while the receiving instances label as 'ch?'. The editor supports graphical and textual representation to create and edit the network of timed automata models. A timed automata model is an instance of a template of the created automaton. UPPAAL timed automata additionally supports aspects of programming languages such as declaring global and/or local variables and function routines. The simulator aids to investigate the dynamic behavior of the system graphically. The sanity functionality can be checked by observing the system traces. The verifier performs the formal verification of the system model against the properties. The queries are the representation of properties under verification. The verifier exhaustively checks the query covering the entire state space of the model. When the property is not satisfied at any of the sampled space, the verifier indicates the result as 'property is not satisfied' implying a bug in the model or query. Formal verification has also been used for modeling and verification of industrial control system (ICS) [39], microgrid [24] and audio protocols [40]. A formal verification of power management is the knowledge gap in design and control of microgrid. The approach presented in this paper bridges the respective gap by using TA for design and verification of the energy management system of a microgrid in the model checker toolbox.

II. Formal Verification Framework for Microgrid Systems

The formal verification framework for microgrid system is represented in Fig. 2. It consists of three main building blocks namely modelling, query formulation and verification. In the modelling stage, a TA model of microgrid system is created through abstraction. The abstraction is carried out by representing microgrid components with suitable states and transitions between the states. For example, the BES component in microgrid system has three states: charging, discharging and idle; and the transition between the states depends on its state-of-charge (SoC), RES and load conditions. The detailed design and modelling of microgrid system is discussed in Section III.

After modelling the microgrid system, queries are formulated for the verification by model checker. Queries are the properties or conditions of the system that should be satisfied by the model. The microgrid system invariants are derived based on allowable and non-allowable operating modes, which are represented as queries. The list of allowable and non-allowable power modes are explained in Section IV. The query language accepted by UPPAAL model checker is timed computation tree logic (TCTL) [35] and so the derived power flow modes are translated to TCTL for verification. The query formulation for microgrid system are explained in Section V. In verification stage, the model checker performs formal verification by

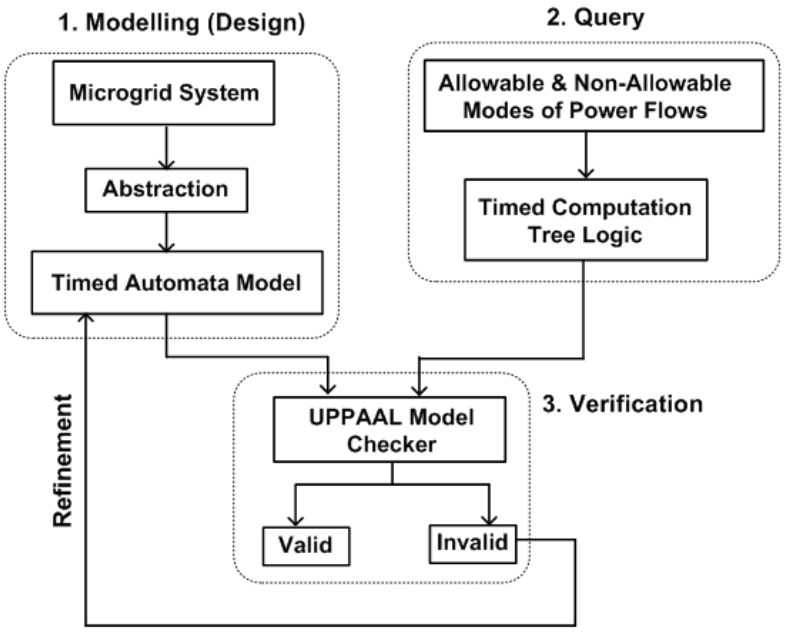

Fig. 2: Formal verification framework for microgrid system.

running the model against queries. The results from the model checker are straightforward i.e., either the query is satisfied or not. If the query is not satisfied, it indicates the presence of design error or query error and it is analysed and corrected in the refinement phase. So the required human effort to check the query is minimum and does not require expertise, though the query formulation may require knowledge about modeling formalism. But once the query is formulated it can be used in future modelling and refinement process. The results from formal verification are discussed in Section VI.

III. Timed Automata Modelling of Microgrid System

The microgrid system considered in this work is illustrated in Fig. 3. It is worthy to mention that the proposed approach is equally applicable to AC microgrids, though the focus in this paper is on DC microgrids. The microgrid system consists of the following components: a PV array, dispatchable unit's such as BES (BES-1 and BES- 2), a diesel generator and a load comprised of residential load, LED lighting and computer racks. The DC energy sources such as PV array and BESes are interfaced via DC-DC converters while the diesel generator is coupled through AC-DC converters. Load is connected to the common DC bus where all energy sources are interfaced together. The BES system has charging and discharging function, and so it is coupled via a bi-directional DC-DC converter.

The status and operation of components are monitored and controlled by the EMS, which is the heart of the microgrid supervisory control system. To efficiently manage the devices, the EMS makes the decisions based on the measurements and load demand. It is designed to accommodate allowable operating modes from energy resources to load, while restricting non-allowable flow of power. This section describes

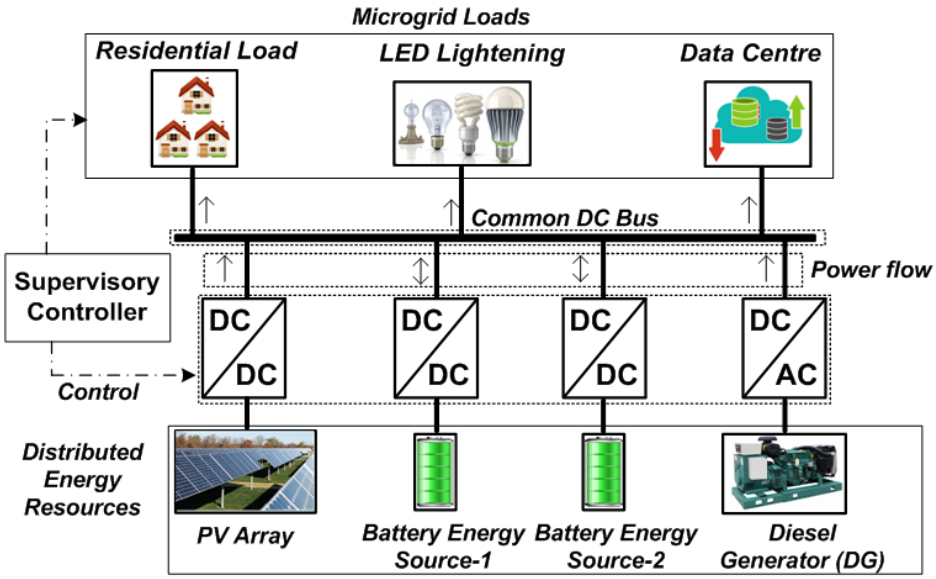

Fig. 3: Overview of a DC microgrid system.

the modeling of individual components in microgrid system. Each component is represented as a TA model based on the dynamics of the components. The models are then interfaced to form a network of TA, through channels and shared variables. The overall energy management system modelled using TA approach is shown in Fig. 4. A detailed description of the components' modelling is presented next.

A. Solar PV system

PV systems are important renewable energy resources and their power generation depends on factors [19] such as solar radiation profile, and cell temperature. To achieve high efficiency, the PV systems should be operated in maximum power point tracking (MPPT) mode, whenever possible. Based on the power generated by the PV and load demand, we have derived three local states of operation for the PV system, as follows:

1) *PV OFF State*: In this state, negligible power is generated from PV due to cloudy, rainy weather, night time, etc.,. In this mode $\text{PV}_{available}$ = 0 and MPPT is turned OFF as well.
2) *MPPT OFF state*: In this mode, the possible PV power generation is larger than the power demand by load and power needed for BES charging. In other words, the power from PV is available but not all of it is needed. Hence, in this mode PV is in ON state and MPPT is in OFF state, $\text{PV}_{available}>0$ & $\text{PV}_{available} > \text{PV}_{consumed}$ and surplus power is limited where $\text{PV}_{consumed}$ is the power consumed from PV.
3) *MPPT ON state*: To extract the maximum power generated by the PV, MPPT is turned ON. The power generated by PV can be utilised to meet load demand or used for BES charging. In short, MPPT is turned ON when $\text{PV}_{available} > 0$ & $\text{PV}_{available} = \text{PV}_{consumed}$.

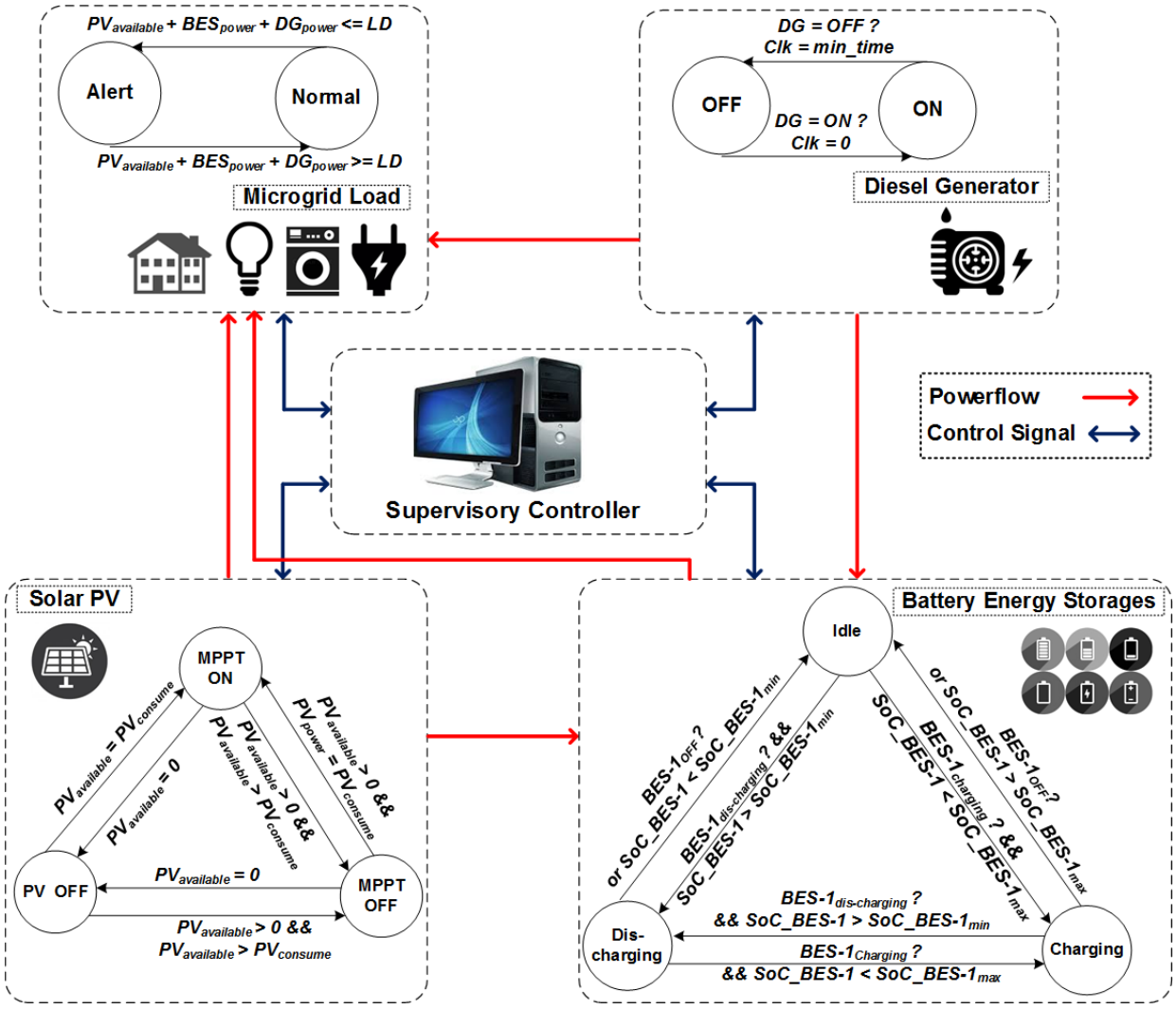

Fig. 4: Overall supervisory energy management system modelling using TA approach.

B. Battery Energy Storage System

To take full advantage of renewable energy sources, it is vital to have a BES capable of handling variations in energy production. In our study, we have considered two BESes in the microgrid system, namely BES-1 and BES-2. The operation of BESes has to be carefully designed and controlled to protect them from damage i.e., over-charging and over-discharging. Maximum and minimum SOC for each BES are derived and set as SOC_BES-1$_{min}$ and SOC_BES-1$_{max}$; and SOC_BES-2$_{min}$ and SOC_BES-2$_{max}$ for BES-1 and BES-2, respectively. To further optimize the battery operation and increase their lifetime, the token technique is implemented [19]. This technique balances the charging and discharging of BESes in the microgrid to safeguard the battery cycle life. Several instructions are involved in this technique to regulate the passing of charging/discharging token, and calculation of SOCs, etc.,. The BESes have three states of operation: idle, charging and discharging. The state transitions of BESes are based on the control decisions determined using SOC of BES, other energy resources in microgrid and load demand.

The controller sends BES-$1_{discharging}$ signal to BES-1 for discharging and so the state transition takes place from idle to discharging state. The BES can supply power until SOC_BES-1 $>$ SOC_BES-1_{min}, after that it is switched to idle state. Likewise, the BES can draw power from microgrid for charging until SOC_BES-1 $<$ SOC_BES-1_{max}, beyond which it transits to idle state. To initiate charging of BES-1, the controller sends BES-$1_{charging}$ signal to BES-1 to transit from idle to charging state. When BES is in idle state, it is neither charging nor discharging.

C. Diesel generator

The reliability and controllability feature of the diesel generator motivates its usage in stand-alone microgrid systems. In the modelling of diesel generator, it is assumed that there is always enough fuel. There are two diesel generator states: OFF and ON. The diesel generator component takes transition from OFF to ON state, only when the available energy resources such as PV and BES combined cannot meet the load demand. To increase the diesel generator efficiency, it is important to optimally control its turn ON/OFF. Maximum power from the diesel generator is harnessed by utilizing its power to charge the BESes. Therefore, the diesel generator is in ON state when the following invariant is satisfied: $\text{PV}_{available}$ + BES_{power} $<$ LD and clk $<$ DG_min_time. Here, clk represents the local clock variable in the diesel generator model and when the transition takes place from OFF to ON state, the clk is reset. $Clock$ is a data-type supported by UPPAAL model checker, which can hold continuous value of evolving time. The diesel generator model transits back to OFF state when $\text{PV}_{available}$ + BES_{power} $>$ LD and clk $>$ DG_min_time.

D. Load

During the islanded mode of operation, the microgrid cannot guarantee continuous power supply to the load since it is often influenced by unpredictable power generation of the PV system. This can be unsafe and overly reliant on the environmental situation, so the system is typically supported with the BES and diesel generator to meet the intermittent nature of renewable energy sources. When the generated power is not able to drive the load, the non-critical loads such as heating, ventilation, and air conditioning (HVAC) in residential loads are shut down.

Nevertheless, a proper design of diesel generator power rating based on the load demand will prevent power outages. Although the model is generic to support both modes, we eliminate this possibility with careful design of diesel generator power rating. Hence, the two operation states of load component are normal and alert mode. The model remains at normal mode when the load demand is met i.e., $\text{PV}_{available}$+ BES_{power} + DG_{power} $\geq$ LD_{power} under any conditions. Similarly, when there is no sufficient power

generation from all the energy resources ($PV_{available}$ + BES_{power} + DG_{power} < LD_{power}), the model is transited to alert mode where non-critical loads are shut down to meet the power requirements of critical load without significant power degradation.

Lastly, it is notable that the model composition derived in this work is scalable. Various energy components can be added, removed, upgraded or duplicated depending on the modelling requirements and topology of microgrid system. Consequently, more system components would add complexity to the model configuration and hence more dependencies would exist. This implies that more computational power is needed to derive the formal verification of a large scale model.

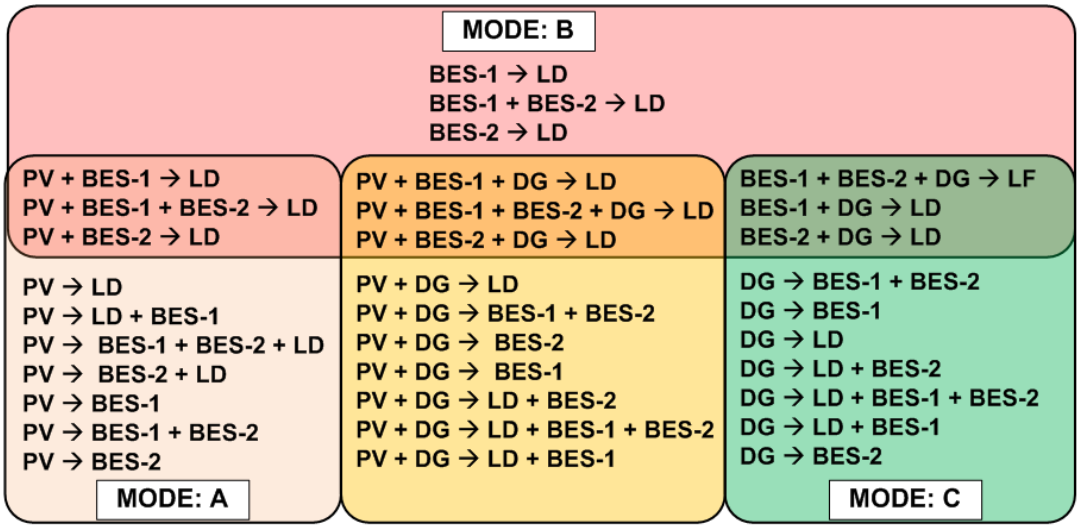

Fig. 5: Allowable modes of operation.

IV. Modes of Operation in Microgrid System

The microgrid system operation is regulated by the centralized EMS. The operating mode in the microgrid system is defined by four important variables:

- $PV_{available}$: Power supplied by PV system
- BES_{power}: Stored battery power in BESes (BES-1 and BES-2)
- DG_{power}: Potential power produced by diesel generator and
- LD_{power}: Power required by the load.

The operating modes in microgrid system are categorized into allowable (Fig. 5) and non-allowable (Table I) modes by identifying all conditions of system operation. They are divided into the following sub-modes based on the available PV power, load power demand and SoC of BES.

Mode A: PV → LD + BES

In this mode, sufficient energy is generated by the PV to drive the load. When the renewable energy generated by PV is equal to load demand i.e., $PV_{available}$ = LD_{power}, PV supplies only to the load. If there is an excess power generated by the PV, it is also possible to charge BESes. The power generated by PV is utilized to supply the load and as well to charge BESes until their respective SOC_BES-1_{max} or SOC_BES-2_{max} is reached.

- PV → LD
- PV → LD + BES-1
- PV → LD + BES-2
- PV → LD + BES-1 + BES-2

In this mode, enabling of an MPPT mode is determined based on the utilization of generated power from PV. When $PV_{available}$ = LD_{power}, the MPPT mode is turned ON. In other cases activation of the MPPT mode is determined depending on the power requirements of load and BES charging.

Mode B: BES → LD

During unforeseen conditions such as cloudy weather or everyday phenomenon such as night time, the energy generated by PV is negligible. So to meet the load demand, the storage devices are used to supply the load. When storage devices have sufficient energy to supply the load, they are discharged until their respective SOC are below the SOC_BES-1_{min} or SOC_BES-2_{min}. There are 3 sub-modes:

- BES-1 → LD
- BES-2 → LD
- BES-1 + BES-2 → LD

The discharging of BES is also operated using co-ordinated discharging as presented in [19]. The EMS selects the suitable BES for discharging based on their respective SOC level to drive the load.

Mode C: DG → LD + BES

When both the renewable energy generation and battery supply are insufficient to drive the load, the diesel generator is used. Although it is not preferable to use diesel generator ; under certain conditions, it is unavoidable to operate microgrid without diesel generator. To efficiently utilize the diesel generator and to extract maximum power, in addition to supplying the load is also used to simultaneously charge the BES. The system may enter into this mode due to insufficient power generation from the PV and energy stored in the BES. Repeated fluctuation in the status of the diesel generator from ON to OFF and vice versa reduces the lifetime and performance of the diesel generator and it has to be handled carefully. To

TABLE I
Non-Allowable operating modes in microgrid system

Sl.No	Non-Allowable operating mode
1	PV + BES-1 $\rightarrow$ LD + BES-2
2	PV + BES-2 $\rightarrow$ LD + BES-1
3	PV + BES-1 $\rightarrow$ BES-2
4	PV + BES-2 $\rightarrow$ BES-1
5	BES-1 $\rightarrow$ BES-2
6	BES-1 $\rightarrow$ LD + BES-2
7	BES-2 $\rightarrow$ BES-1
8	BES-2 $\rightarrow$ LD + BES-1
9	DG + BES-1 $\rightarrow$ BES-2
10	DG + BES-1 $\rightarrow$ LD + BES-2
11	DG + BES-2 $\rightarrow$ BES-1
12	DG + BES-2 $\rightarrow$ BES-1 + LD
13	PV + DG + BES-1 $\rightarrow$ BES-2
14	PV + DG + BES-1 $\rightarrow$ BES-2 + LD
15	PV + DG + BES-2 $\rightarrow$ BES-1
16	PV + DG + BES-2 $\rightarrow$ BES-1 + LD

avoid this fluctuation, the invariants for diesel generator operation are utilized. An invariant is a condition which has to hold in this system regardless of operation sequence. Diesel generator has to be in the ON state for minimum operation duration (DG_min_time) before it can transit back to OFF state. So the diesel generator can switch to OFF state only when DG_min_time has been passed and there is sufficient power generated from PV and BES to supply the load i.e., $\text{PV}_{available}$ + $\text{BES}_{power} > \text{LD}_{power}$ & clk $>$ DG_min_time.

Following sub-modes are used in the diesel generator operation

- DG $\rightarrow$ Load
- DG $\rightarrow$ Load + BES-1
- DG $\rightarrow$ Load + BES-2
- DG $\rightarrow$ Load + BES-1 + BES-2

Mode D: BES $\rightarrow$ LD + BES

It is possible to include energy flow where one of the BES is discharged to charge another BES (and supply the load). This mode is excluded to prevent inefficient operation of BES i.e., to maximize productivity of BES in this model. A list of non-allowable modes i.e., restricted operating modes are tabulated in Table I.

The correctness of a system design lies in proper verification of system properties. Hence the testing of operating modes with high confidence is essential for both allowable and non-allowable operating modes.

So the main focus of this work is on technique to verify the modes rather than the choices of component parameters such as DG_min_time or SOC_BES-1$_{min}$.

TABLE II
TCTL Expression in UPPAAL Verifier

Query	**Description**	**Property**
`A [] Q`	For all paths, Q always holds	Invariantly (Q is true in all reachable states)
`E [] Q`	There exists a path where Q always holds	Potentially always (Q is true in all reachable states of (at least) one path)
`A <> Q`	For all paths, Q will eventually hold	Eventually (Q is true in some state of all paths)
`E <> Q`	There exists a path where Q will eventually hold	Possibly (Q is true in (at least) one reachable state)
`P imply Q`	For any path, whenever P holds true, Q also holds	Leads to (In all paths, if P becomes true, Q will inevitably hold)
`P` $\rightarrow$ `Q`	For any path, if P holds then Q will also holds eventually	Leads to (P lead to Q)

P and Q refer to the property for verification

V. UPPAAL Query Formulation for Microgrid System

The conditions or the properties to be verified against the model in UPPAAL are expressed as queries in the form of TCTL expressions. Table II lists the TCTL expressions used in UPPAAL verifier. In this work, the queries define the operating mode conditions to be tested against the developed microgrid model. The properties defined in TCTL form are interpreted over computation tree evolving along time by unfolding the state machine in the form of a tree. As seen in Table II, there are two path qualifiers (E and A) along with temporal operators. The notation E represents the 'existential' and A represents the 'universal' path qualifier.

- The property (P) expressed by $A[]P$ is satisfied, if and only if P is true on all runs of state space. The universal path qualifiers can be expressed to verify the safety conditions of the system.
- The property (Q) expressed by $E <> Q$ is satisfied, if Q holds true on some runs of state space. The existential path qualifiers can be expressed to verify the reachability conditions in the system.

The query $A[]\ not\ deadlock$ checks if the process does not contain any deadlocks. It is a useful feature to verify if the modeled system is correct without any deadlock especially for control algorithms. With conventional approaches, the deadlock property verification is not well defined. In this work, both allowable and non-allowable operating modes and transitions are expressed as queries and verified in UPPAAL verifier. The verification of the power flow modes is performed against the designed microgrid model. A few of the verification queries for microgrid system are presented in Table III.

VI. Result Discussion : Simulation & Formal Verification

A. Conventional Simulation based verification

A detailed discussion of simulation results is given below for verification of allowable operating modes of microgrid. The specification of the designed microgrid system is as follows: DG = 10 kW, BES-1 & BES-2 = 4 kW, PV = 8 kW and load = 8 kW. This study is carried out to observe allowable operating modes in the microgrid by controlling the $\text{PV}_{available}$ and the LD_{power}.

Fig. 6 shows the simulation results of microgrid modes of operation transiting from allowable to non-allowable mode. When t = 0 to 7s, load is oscillating from 7 kW to 8 kW to meet the demand. PV, BES-1 and BES-2 power are co-ordinated to achieve power balance among load and power source. During the time interval t = 7 to 13s, the load value is still between 7 kW to 8 kW, power from PV system and BES-2 supplies to load to meet the demand, parallel charging of BES-1 causes the power imbalance between load and power source, this transits the microgrid mode operation from allowable to non-allowable mode. Fig. 6 (b) shows the common DC bus voltage tracking response, in normal mode DC link voltage follows the reference voltage. As soon as the microgrid transits to non-allowable mode, DC link voltage drops down from the reference voltage and this could cause system black out.

In the conventional simulation verification approach, following limitations are inferred:

- An expert knowledge is required to analyse the correctness of the results. As seen in Fig. 6, during interval t = 8-12s, it can be observed that BES-2 is discharged to supply the load and BES-1 charging, which is a non-allowable mode. In manual analysis, this condition may be overlooked and the design error may be left unidentified.
- It is not possible to verify modes under all possible conditions i.e., in one simulation run, the property is only verified for a particular scenario. For e.g., in Fig. 6, though discharging of BES is simulated with $\text{PV}_{available}$ being available, the expected discharging behavior with negligible $\text{PV}_{available}$ was not guaranteed.
- Non-allowable scenarios are not verifiable with confidence using the simulation technique. For e.g., BES-1 discharging to charge BES-2 is not verified in simulation.

B. Formal Verification of Microgrid system

In formal verification approach, the TA model of microgrid system and their corresponding operating mode queries are tested in the UPPAAL model checker. This approach explores the state space of the microgrid system model to check if the queries are satisfied or not i.e., it verifies the correctness of microgrid system model. When the query for an allowable operating mode is not-satisfied or when a query for a non-allowable operating mode is satisfied; then there is a design error present in the system

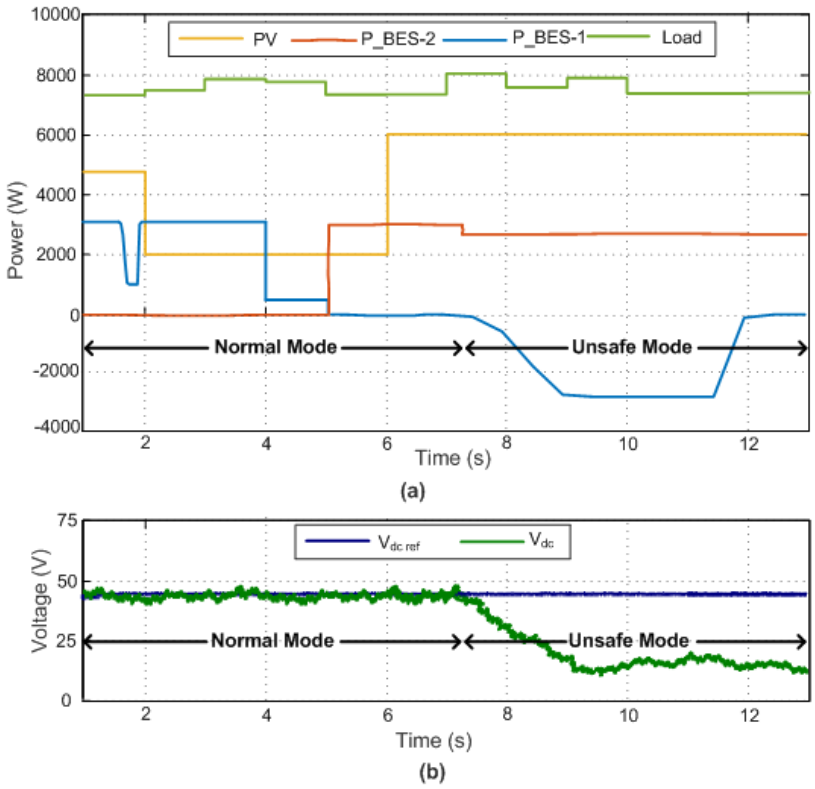

Fig. 6: Allowable mode to non-allowable mode

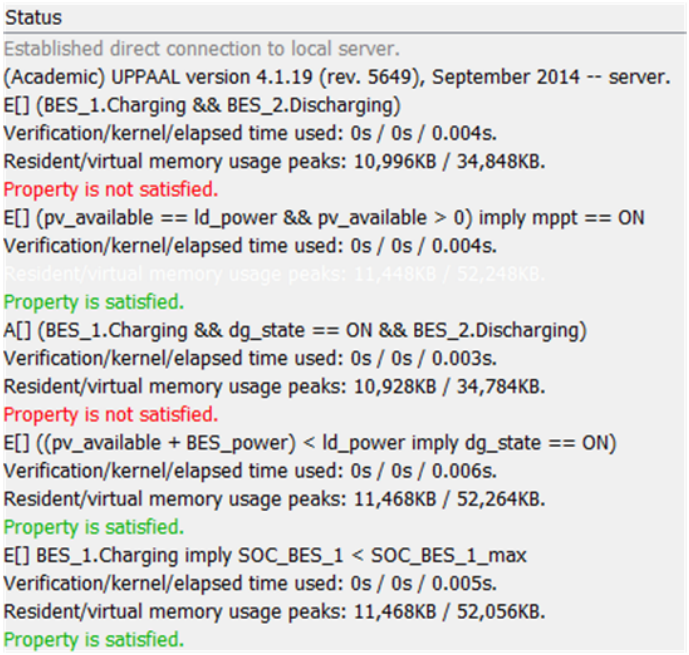

Fig. 7: Screenshot of UPPAAL verification status of microgrid queries

model. The corresponding failed query is analyzed to correct the TA model of microgrid in the refinement phase. All the allowable and non-allowable modes are translated to UPPAAL queries expressed as TCTL as discussed in Section V. A few of queries used in verification of microgrid are also presented in Table III. For instance, a non-allowable condition from mode D i.e., BES-2 $\rightarrow$ BES-1 is translated to UPPAAL query

as `E<> (BES-1.Charging && BES-2.Discharging)`. This query verifies that if this condition is present in the state space of the model. During verification of the query against microgrid model, the non-allowable operating mode condition was not satisfied i.e., it did not exist in the design of microgrid inferring that the design was correct.

Both allowable and non-allowable queries are verified with high confidence using formal verification. Since the verifier explores the complete state space, the query condition is guaranteed under all possible scenarios. A screenshot of verification queries executed in UPPAAL model checker is presented in Fig. 7. Though the query formulation requires expert knowledge, the query execution and result analysis does not require expertise. Once formulated query can also be used again to check the conditions after refinement of the model.

C. Discussion

From this analysis of simulation based verification and formal verification, a few discussion points are presented here. Different aspects are considered to assess the model verification technique such as assurance of design correctness, ease of analyzing the results and coverage of modes.

a) Assurance to design correctness: In the simulation based verification technique, the assurance of design correctness was weak. Since both simulation and formal verification rely on system model i.e., abstraction of system, the probability of model error misleading the verification results are the same in both the techniques. But the formal verification through model checker verifies the properties by checking entire state space of the system. While simulation verification can check the properties specific to behavior of system under an input i.e. the property may fail to hold in the system with different input as the simulation trace could be different.

b) Ease of analyzing the results: Simulation of system under possible input to validate a property could be practically time consuming and requires more computational or human effort. The need of knowledge to test and analyse the result by providing required input and analyzing the expected simulation results is also one of the setbacks in simulation based verification. Though the query formation is crucial and the correctness of query is essential to appreciate the results, the effort involved in query formation is minimal; as a query once developed can be used to verify against multiple versions of the model.

c) Coverage of modes: The allowable operating modes were able to be simulated by providing suitable inputs by which the system was made to follow a simulation path. However, the simulation verification results correspond to the correctness of modes of operation respective to the environment setting and the simulated inputs. So the guarantee of the mode in other setting or inputs may not be true. The model checker verifies the mode of operation exhaustively through the entire state space. The

non-allowable modes were not verifiable in simulation based verification, while in formal verification, suitable queries were formulated to test and verify those modes.

d) Shortcomings of formal verification: Both the modeling procedure and the verification which is done by the formal method have their shortcomings. In general every system that has states and transitions between the states can be checked using the model checker. Therefore, the user needs to identify the components of his system and model them as TA. The components of the microgrid and the control algorithm can easily be transferred to TA models because of their discrete nature. However, if the number of locations of the TA increases, the size of the state space that needs to be checked is increased i.e. we are facing the state space explosion problem [41]. When the number of state variables increases in the system, the state space grows exponential in size. Recently, solutions to state space explosion have been proposed in [42]–[44] to make the technique more practical for real-world systems. The other negative aspect is that formal verification can only be applied to finite state systems. A system with infinite states can be abstracted to finite state with a trade-off on the precision on the system model. The other shortcomings of formal verification is deriving specifications. It requires knowledge on temporal specifications to verify the system. Though property to verify is checked under entire state space, the correctness and effectiveness of the properties ought to be studied to completely verify the system. An error in specification could also lead to incorrect verification results where the system may still have faults.

VII. Conclusion

This paper presents the modelling and verification of a supervisory energy management system by formulating invariants for possible mode change in microgrid system. A timed automata network model of the microgrid was designed by modelling the dynamics of the components such as PV, BES, diesel generator, load and controller. The states and transitions between the states are abstracted to derive the model. The BESes were designed with the ability of charging and discharging. The possible modes of operation in the microgrid between the energy sources and load are derived and categorized to allowable and non-allowable operating modes. The non-allowable operating modes are counter-productive flows decreasing the microgrid reliability. Verification was performed on the designed microgrid models based on simulation and formal methods. To perform simulation based verification, the designed model was subjected to various inputs and tested for expected behavior. Formal verification was conducted using UPPAAL model checker. Queries are derived for allowable and non-allowable operating modes to verify the design of microgrid. The queries are validated against the TA model of microgrid and the observed results are presented. From the presented study, it can be observed that formal verification approach is effective for reliable design verification guaranteeing correctness of design for stable and efficient operation of microgrid.

REFERENCES

[1] M. Bragard, N. Soltau, S. Thomas, and R. W. De Doncker, "The balance of renewable sources and user demands in grids: Power electronics for modular battery energy storage systems," *IEEE Trans. Power Electron.*, vol. 25, no. 12, pp. 3049–3056, 2010.

[2] J. M. Carrasco, L. G. Franquelo, J. T. Bialasiewicz, E. Galván, R. C. PortilloGuisado, M. M. Prats, J. I. León, and N. Moreno-Alfonso, "Power-electronic systems for the grid integration of renewable energy sources: A survey," *IEEE Trans. Ind. Electron.*, vol. 53, no. 4, pp. 1002–1016, 2006.

[3] K. Sun, X. Wang, Y. W. Li, F. Nejabatkhah, Y. Mei, and X. Lu, "Parallel operation of bidirectional interfacing converters in a hybrid ac/dc microgrid under unbalanced grid voltage conditions," *IEEE Trans. Power Electron.*, vol. 32, no. 3, pp. 1872–1884, 2017.

[4] Y. Xia, Y. Peng, P. Yang, M. Yu, and W. Wei, "Distributed coordination control for multiple bidirectional power converters in a hybrid ac/dc microgrid," *IEEE Trans. Power Electron.*, vol. 32, no. 6, pp. 4949–4959, 2017.

[5] T. Dragičević, X. Lu, J. C. Vasquez, and J. M. Guerrero, "Dc microgrids - part i: A review of control strategies and stabilization techniques," *IEEE Trans. Power Electron.*, vol. 31, no. 7, pp. 4876–4891, July 2016.

[6] ——, "Dc microgrids - part II : A review of power architectures, applications, and standardization issues," *IEEE Trans. Power Electron.*, vol. 31, no. 5, pp. 3528–3549, May 2016.

[7] E. Barklund, N. Pogaku, M. Prodanovic, C. Hernandez-Aramburo, and T. C. Green, "Energy management in autonomous microgrid using stability-constrained droop control of inverters," 2008.

[8] J. P. Lopes, C. Moreira, and A. Madureira, "Defining control strategies for microgrids islanded operation," *IEEE Transactions on power systems*, vol. 21, no. 2, pp. 916–924, 2006.

[9] F. Katiraei and M. R. Iravani, "Power management strategies for a microgrid with multiple distributed generation units," *IEEE transactions on power systems*, vol. 21, no. 4, pp. 1821–1831, 2006.

[10] H. S. V. S. K. Nunna and S. Doolla, "Multiagent-based distributed-energy-resource management for intelligent microgrids," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 4, pp. 1678–1687, April 2013.

[11] S.-J. Ahn, J.-W. Park, I.-Y. Chung, S.-I. Moon, S.-H. Kang, and S.-R. Nam, "Power-sharing method of multiple distributed generators considering control modes and configurations of a microgrid," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, pp. 2007–2016, 2010.

[12] D. Dong, T. Thacker, I. Cvetkovic, R. Burgos, D. Boroyevich, F. Wang, and G. Skutt, "Modes of operation and system-level control of single-phase bidirectional pwm converter for microgrid systems," *IEEE Transactions on Smart Grid*, vol. 3, no. 1, pp. 93–104, March 2012.

[13] F. Valenciaga and P. F. Puleston, "Supervisor control for a stand-alone hybrid generation system using wind and photovoltaic energy," *IEEE Transactions on Energy Conversion*, vol. 20, no. 2, pp. 398–405, June 2005.

[14] C. K. Sao and P. W. Lehn, "Control and power management of converter fed microgrids," *IEEE Transactions on Power Systems*, vol. 23, no. 3, pp. 1088–1098, Aug 2008.

[15] M. Kumar, S. C. Srivastava, and S. N. Singh, "Control strategies of a dc microgrid for grid connected and islanded operations," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1588–1601, July 2015.

[16] W.-J. Ma, J. Wang, X. Lu, and V. Gupta, "Optimal operation mode selection for a dc microgrid," *IEEE Trans. Smart Grid*, vol. 7, no. 6, pp. 2624–2632, 2016.

[17] N. Korada and M. K. Mishra, "Grid adaptive power management strategy for an integrated microgrid with hybrid energy storage," *IEEE Trans. Ind. Electron.*, vol. 64, no. 4, pp. 2884–2892, 2017.

[18] S. Kotra and M. K. Mishra, "A supervisory power management system for a hybrid microgrid with hess," *IEEE Trans. Ind. Electron.*, vol. 64, no. 5, pp. 3640–3649, 2017.

[19] T. Dragičević, J. M. Guerrero, J. C. Vasquez, and D. Škrlec, "Supervisory control of an adaptive-droop regulated dc microgrid with battery management capability," *IEEE Trans. Power Electron.*, vol. 29, no. 2, pp. 695–706, 2014.

[20] G. Faraut, L. Piétrac, and E. Niel, "Formal approach to multimodal control design: Application to mode switching," *IEEE Trans. Ind. Informat*, vol. 5, no. 4, pp. 443–453, 2009.

[21] A. Ovalle, G. Ramos, S. Bacha, A. Hably, and A. Rumeau, "Decentralized control of voltage source converters in microgrids based on the application of instantaneous power theory," *IEEE Trans. Ind. Electron.*, vol. 62, no. 2, pp. 1152–1162, Feb 2015.

[22] S. Bracco, M. Brignone, F. Delfino, and R. Procopio, "An energy management system for the savona campus smart polygeneration microgrid," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1799–1809, Sept 2017.

[23] G. Kunz, J. Machado, E. Perondi, and V. Vyatkin, "A formal methodology for accomplishing iec 61850 real-time communication requirements," *IEEE Trans. Ind. Electron.*, vol. 64, no. 8, pp. 6582–6590, Aug 2017.

[24] G. Sugumar, R. Selvamuthukumaran, T. Dragicevic, U. Nyman, K. G. Larsen, and F. Blaabjerg, "Formal validation of supervisory energy management systems for microgrids," in *Industrial Electronics Society, IECON 2017-43rd Annual Conference of the IEEE*. IEEE, 2017, pp. 1154–1159.

[25] B. F. Adiego, D. Darvas, E. B. Viuela, J. C. Tournier, S. Bliudze, J. O. Blech, and V. M. G. Surez, "Applying model checking to industrial-sized plc programs," *IEEE Trans. Ind. Electron.*, vol. 11, no. 6, pp. 1400–1410, Dec 2015.

[26] L. Benini, A. Bogliolo, and G. De Micheli, "A survey of design techniques for system-level dynamic power management," *IEEE transactions on very large scale integration (VLSI) systems*, vol. 8, no. 3, pp. 299–316, 2000.

[27] K. Havelund, K. G. Larsen, and A. Skou, "Formal verification of a power controller using the real-time model checker uppaal," in *International AMAST Workshop on Aspects of Real-Time Systems and Concurrent and Distributed Software*. Springer, 1999, pp. 277–298.

[28] D. Kalita and P. P. Khargonekar, "Formal verification for analysis and design of logic controllers for reconfigurable machining systems," *IEEE transactions on Robotics and Automation*, vol. 18, no. 4, pp. 463–474, 2002.

[29] J. Suryadevara, G. Sapienza, C. Seceleanu, T. Seceleanu, S.-E. Ellevseth, and P. Pettersson, "Wind turbine system: An industrial case study in formal modeling and verification," in *International Workshop on Formal Techniques for Safety-Critical Systems*. Springer, 2013, pp. 229–245.

[30] B. Wu, M. D. Lemmon, and H. Lin, "Formal methods for stability analysis of networked control systems with ieee 802.15. 4 protocol," *IEEE Transactions on Control Systems Technology*, vol. 26, no. 5, pp. 1635–1645, 2018.

[31] M. Střelec, K. Macek, and A. Abate, "Modeling and simulation of a microgrid as a stochastic hybrid system," in *Innovative Smart Grid Technologies (ISGT Europe), 2012 3rd IEEE PES International Conference and Exhibition on*. IEEE, 2012, pp. 1–9.

[32] K. G. Larsen, P. Pettersson, and W. Yi, "Uppaal in a nutshell," *International Journal on Software Tools for Technology Transfer*, vol. 1, no. 1-2, pp. 134–152, 1997.

[33] T. A. Henzinger, "The theory of hybrid automata," in *Verification of Digital and Hybrid Systems*. Springer, 2000, pp. 265–292.

[34] K. Havelund, A. Skou, K. G. Larsen, and K. Lund, "Formal modeling and analysis of an audio/video protocol: An industrial case study using uppaal," in *Real-Time Systems Symposium, 1997. Proceedings., The 18th IEEE*. IEEE, 1997, pp. 2–13.

[35] T. Hune, K. G. Larsen, and P. Pettersson, "Guided synthesis of control programs using uppaal," *Nordic J. of Computing*, vol. 8, pp. 43–64, 2001.

[36] G. Gardey, D. Lime, M. Magnin *et al.*, "Romeo: A tool for analyzing time petri nets," in *International Conference on Computer Aided Verification*. Springer, 2005, pp. 418–423.

[37] M. Kwiatkowska, G. Norman, and D. Parker, "Prism: Probabilistic symbolic model checker," in *International Conference on Modelling Techniques and Tools for Computer Performance Evaluation*. Springer, 2002, pp. 200–204.

[38] G. J. Holzmann, "The model checker spin," *IEEE Trans. Software Engineering*, vol. 23, no. 5, pp. 279–295, 1997.

[39] G. Sugumar and A. Mathur, "Testing the effectiveness of attack detection mechanisms in industrial control systems," in *Software Quality, Reliability and Security Companion (QRS-C), 2017 IEEE International Conference on*. IEEE, 2017, pp. 138–145.

[40] J. Bengtsson, W. D. Griffioen, K. J. Kristoffersen, K. G. Larsen, F. Larsson, P. Pettersson, and W. Yi, "Verification of an audio protocol with bus collision using uppaal," in *International Conference on Computer Aided Verification*. Springer, 1996, pp. 244–256.

[41] E. M. Clarke, W. Klieber, M. Nováček, and P. Zuliani, "Model checking and the state explosion problem," in *Tools for Practical Software Verification*. Springer, 2012, pp. 1–30.

[42] O. Grumberg and H. Veith, *25 years of model checking: history, achievements, perspectives*. Springer, 2008, vol. 5000.

[43] W. Chan, R. J. Anderson, P. Beame, D. H. Jones, D. Notkin, and W. E. Warner, "Decoupling synchronization from local control for efficient symbolic model checking of statecharts," in *Proceedings of the 21st international conference on Software engineering*. ACM, 1999, pp. 142–151.

[44] K. L. McMillan, "Symbolic model checking," in *Symbolic Model Checking*. Springer, 1993, pp. 25–60.

TABLE III
Queries for Allowable & Non-Allowable Modes Verification of Microgrid System

Condition	**Description**	**Query**
BES-2 → BES-1 (Non-Allowable operating mode)	It is a representation of a non-allowable operating mode verified in UPPAAL model checker. This query verifies that when BES-1 is in the charging mode, the other BES-2 should not be in the discharging mode. The operating mode from one BES to other BES in a microgrid system is counter-productive and may damage the BES system.	`E[] (BES_1.Charging && BES_2.Discharging)`
PV → LD (Allowable operating mode)	The query is used to verify that the MPPT mode is turned ON, when the power from the PV is fully utilized to meet the load demand.	`E[] (pv_available == ld_power && pv_available > 0) imply mppt == ON`
BES-2 → DG + BES-1 (Non-Allowable operating mode)	A non-allowable operating mode from BES-2 and diesel generator to charge BES-1 is verified with this query. There should not be any scenario in microgrid design, where power from diesel generator and one BES is used to charge the other BES.	`A[] (BES_1.Charging && dg_state == ON && BES_2.Discharging)`
PV + BES-1 + BES-2 + DG → LD (Allowable operating mode)	An allowable mode where power from PV and BES are negligible, the diesel generator is turned ON to drive load.	`E[] ((pv_available + BES_power) < ld_power imply dg_state == ON)`
BES charging until SOC_BES$_{max}$	The charging process of BES should not be continued after reaching maximum allowable SOC.	`EE[] BES_2.Charging imply SOC_BES_2 < SOC_BES_2_max` `E[] BES_1.Charging imply SOC_BES_1 < SOC_BES_1_max`
BES discharging until SOC_BES$_{min}$	The query verifies that the discharge of the BES-1 is performed when the SOC of corresponding BES is within the safe limits of the SOC. When the BES-1 is in discharging state, the SOC of BES-1 should always remain higher than the SOC_BES-1$_{min}$.	`E[] BES_1.Charging imply SOC_BES_1 < SOC_BES_1_max`
PV + BES-1 → BES-1 (Non-Allowable operating mode)	This query verifies if the power discharged from BES-2 and PV power is utilized to charge the BES-1. It is a non-allowable operating mode (Mode D) and the query was not satisfied during the verification of the microgrid model in UPPAAL.	`E<> (BES_2.Discharging && MPPT == ON && BES_1.Charging)`
PV → LD + BES-1 (Allowable operating mode)	The verifier checks the existence of a path when the generated PV power is higher than the load demand and the excess power from the PV is utilized to charge the BES. The charging of the BES is performed only when its SOC is lower than the SOC_BES-1$_{max}$.	`E[] (pv_available > ld_power imply BES_1.Charging)`
Deadlock Condition	Query to verify if deadlock exist in the system model	`A[] not deadlock`